Anwenderhandbuch

TAINY HMOD-V3-IO, TAINY HMOD-L3-IO
TAINY EMOD-V3-IO, TAINY EMOD-L3-IO
Produktvariante DS
Produktvariante E5







Dr. Neuhaus Telekommunikation GmbH

Papenreye 65, D-22453 Hamburg

Fax.: +49 (40) 55304-180

Internet: http://www.neuhaus.de

E-Mail: Kundendienst@neuhaus.de

Technische Änderungen vorbehalten.

TAINY® ist ein Warenzeichen der Dr. Neuhaus Telekommunikation GmbH. Alle anderen Warenzeichen und Produktbezeichnungen sind Warenzeichen, eingetragene Warenzeichen oder Produktbezeichnungen der jeweiligen Inhaber.

Alle Lieferungen und Leistungen erbringt die Dr. Neuhaus Telekommunikation GmbH auf der Grundlage der Allgemeinen Geschäftsbedingungen der Dr. Neuhaus Telekommunikation GmbH in der jeweils aktuellen Fassung. Alle Angaben basieren auf Herstellerangaben. Keine Gewähr oder Haftung bei fehlerhaften und unterbliebenen Eintragungen. Die Beschreibungen der Spezifikationen in diesem Handbuch stellen keinen Vertrag da.

Produkt-Nr.: 3196

Dok.-Nr.: 3196AD003 Version 1.5

Produkte: TAINY HMOD-V3-IO, TAINY EMOD-V3-IO

TAINY HMOD-L3-IO, TAINY EMOD-L3-IO

inkl. Produktvariante E5, Produktvariante DS

Ab Firmware-Version 2.605



Sicherheitshinweise

Produkte

Die Bezeichnung TAINY xMOD wird im Folgenden als Sammelbegriff für das TAINY HMOD-V3-IO, TAINY HMOD-L3-IO, TAINY EMOD-V3-IO, TAINY EMOD-L3-IO sowie die Produktvarianten E5 (5-Port-Ethernet-Switch) und DS (Dual SIM) verwendet.

Qualifiziertes Personal

Das zugehörige Gerät/System darf nur in Verbindung mit dieser Dokumentation eingerichtet und betrieben werden. Inbetriebsetzung und Betrieb eines Gerätes/Systems dürfen nur von qualifiziertem Personal vorgenommen werden. Qualifiziertes Personal im Sinne der sicherheitstechnischen Hinweise dieser Dokumentation sind Personen, die die Berechtigung haben, Geräte, Systeme und Stromkreise gemäß den Standards der Sicherheitstechnik in Betrieb zu nehmen, zu erden und zu kennzeichnen.

Allgemeine Hinweise zu dem Produkt

Das Produkt TAINY xMOD entspricht der europäischen Norm EN60950 (11.2006 /A1:2010), Einrichtungen der Informationstechnik - Sicherheit. Lesen Sie vor Gebrauch des Gerätes die Installationsanleitung sorgfältig durch. Halten Sie das Gerät von Kindern fern, besonders von Kleinkindern. Das Gerät darf nicht im Freien oder in Feuchträumen installiert und betrieben werden. Nehmen Sie das Gerät nicht in Betrieb, wenn Anschlussleitungen oder das Gerät selbst beschädigt sind.

Externe Stromversorgung

Verwenden Sie nur eine externe Stromversorgung die ebenfalls der EN60950 entspricht. Die Ausgangsspannung der externen Stromversorgung darf 60V DC nicht überschreiten. Der Ausgang der externen Stromversorgung muss kurzschlussfest sein.

Das TAINY xMOD darf nur aus Stromversorgungen nach IEC/EN60950 Abschnitt 2.5 "Stromquelle mit begrenzter Leistung" versorgt werden. Die externe Stromversorgung für das TAINY xMOD muss den Bestimmungen für NEC Klasse 2 Stromkreisen entsprechen, wie im National Electrical Code ® (ANSI/NFPA 70) festgelegt.

Bei Anschluss an eine Batterie oder einen Akkumulator beachten Sie, dass zwischen dem Gerät und der Batterie oder Akkumulator eine allpolige Trennvorrichtung (Batteriehauptschalter) mit ausreichendem Trennvermögen sowie eine Sicherung mit ausreichendem Trennvermögen vorzusehen sind (z. B. Pudenz FKS Sicherungssatz 32 V, 3 A, Best.-Nr. 162.6185.430).

Beachten Sie den Abschnitt Technische Daten dieser Dokumentation (Kapitel 17) sowie die Einbau- und Nutzungsvorschriften des jeweiligen Herstellers der Stromversorgung, der Batterie oder des Akkumulators.

Schalteingang und Schaltausgang

Der Schalteingang und der Schaltausgang sind jeweils gegenüber den anderen Anschlüssen des TAINY xMOD galvanisch getrennt. Verbindet die am TAINY xMOD angeschlossene Installation ein Signal des Schalteingangs oder des Schaltausgangs galvanisch mit der Versorgungsspannung, darf zwischen jedem Signal des Schalteingangs oder des Schaltausgangs und jedem Anschluss der Versorgungsspannung des TAINY xMOD die Spannung jeweils 60V nicht überschreiten.

Umgang mit Kabeln

Ziehen Sie niemals einen Kabelstecker am Kabel aus seiner Buchse, sondern ziehen Sie am Stecker. Führen Sie die Kabel nicht ohne Kantenschutz über scharfe Ecken und Kanten. Sorgen Sie gegebenenfalls für eine ausreichende Zugentlastung der Kabel. Achten Sie bitte darauf, dass aus Sicherheitsgründen der Biegeradius der Kabel eingehalten wird. Die Nichteinhaltung der Biegeradien des Antennenkabels führt zu Verschlechterung der Sende- und Empfangseigenschaften des Gerätes. Der minimale Biegeradius darf statisch den 5-fachen Kabeldurchmesser und dynamisch den 15-fachen Kabeldurchmesser nicht unterschreiten.

Funkgerät

Verwenden Sie das Gerät niemals in Bereichen, in denen der Betrieb von Funkeinrichtungen untersagt ist. Das Gerät enthält einen Funksender, der gegebenenfalls medizinische elektronische Geräte wie Hörgeräte oder Herzschrittmacher in ihrer Funktion beeinträchtigen kann. Ihr Arzt oder der Hersteller solcher Geräte können Sie beraten. Damit keine Datenträger entmagnetisiert werden, lagern Sie bitte keine Disketten, Kreditkarten oder andere magnetische Datenträger in der Nähe des Gerätes.

Antennen-Montage

Das Einhalten der empfohlenen Strahlungsgrenzwerte der Strahlenschutzkommission vom 13./14. September 2001 muss gewährleistet sein.

Montage einer Außenantenne

Bei der Installation einer Antenne im Freien ist es zwingend erforderlich, dass die Antenne durch eine Fachkraft montiert wird. Die Einhaltung der Blitzschutznorm DIN EN 62305 Teil 1 bis 4 in ihrer aktuellen Fassung und weiterführende Normen sind dabei vorgeschrieben.

Das EMV Blitzschutzzonen-Konzept nach EN 62305-4

Das Blitzschutzzonen-Konzept ist einzuhalten. Um große Induktionsschleifen zu vermeiden, ist ein Blitzschutz-Potentialausgleich anzuwenden. Werden Antenne oder Antennenkabel in der Nähe der Blitzschutzanlage montiert, müssen die Mindestabstände zur Blitzschutzanlage eingehalten werden. Ist dies nicht möglich, ist eine isolierte Montage wie in der Blitzschutznorm DIN EN 62305 Teil 1 bis 4, in ihrer aktuellen Fassung beschrieben, zwingend erforderlich.



HF-Exposition

Normalerweise arbeitet die am Sender dieses Gerätes angeschlossene Antenne in allen Richtungen mit 0 dB Verstärkung. Die Composite Power im PCS-Modus ist bei Benutzung dieser Antenne geringer als 1 Watt ERP.

Die mit diesem mobilen Gerät benutzen internen / externen Antennen müssen mindestens 20 cm von Personen entfernt sein. Und sie dürfen nicht so platziert oder betrieben werden, dass sie in Verbund mit einer anderen Antenne oder Sender arbeiten.



Funkstörungen

Das TAINY xMOD ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.



Vorsicht, Kosten!

Bitte beachten Sie, dass auch beim (Wieder-) Aufbau einer Verbindung, bei Verbindungsversuchen zur Gegenstelle (z.B. Server ausgeschaltet, falsche Zieladresse, etc.) sowie zum Erhalt einer Verbindung kostenpflichtige Datenpakete ausgetauscht werden. So kann zum Beispiel eine nicht erreichbare Gegenstelle dazu führen, dass durch misslungene Versuche beim Verbindungsaufbau zusätzliche Kosten entstehen.

Firmware mit Open Source GPL/LGPL

Die Firmware von TAINY xMOD enthält open Source Software unter GPL/LGPL Bedingungen. Gemäß des Abschnitts 3b von GPL und des Abschnitts 6b von LGPL bieten wir Ihnen den Quellkode an. Sie finden den Quellkode auf unserer Web-Seite im Internet www.neuhaus.de.

Alternativ können Sie den Quellkode auch bei uns auf CD-ROM anfordern. Senden Sie eine E-Mail an Kundendienst@neuhaus.de. Als Betrifftext Ihrer E-Mail geben Sie bitte 'Open Source xMOD' an, um Ihre Nachricht leicht herausfiltern zu können.

Die Lizenzbedingungen der open Source Software erhalten Sie mit dem Quellkode.

Firmware mit OpenBSD

Die Firmware von TAINY xMOD enthält Teile aus der OpenBSD-Software. Die Verwendung von OpenBSD-Software verpflichtet zum Abdruck des folgenden Copyright-Vermerkes:

Ein Wort von unserem Technischen Kundendienst

Wir, die Techniker des Kundendienstes der Dr. Neuhaus Telekommunikation GmbH, begrüßen Sie recht herzlich. Sollten Sie bei der Inbetriebnahme Ihres neuen Geräts Schwierigkeiten haben, sind wir Ihre Ansprechpartner, und wir helfen Ihnen gern. Auch bei speziellen und ungewöhnlichen Konstellationen in Hardware und Software werden Sie bei uns immer ein offenes Ohr finden, wenn einmal nicht alles sofort klappen will. Der gute Ruf unserer Produkte beruht auch darauf, dass unseren Kunden stets ein Team kundiger Fachleute zur Verfügung steht, das sich auch auf ungewöhnliche Konstellationen einlässt. Sie erreichen uns unter **Kundendienst@neuhaus.de**.

Umweltschutz ist auch unser Thema

Der Erhalt einer lebenswerten Umwelt, d.h. die sinnvolle Verknüpfung von Ökologie und Ökonomie, ist eine der wichtigsten Aufgaben unserer Zeit. Wir begegnen dieser Herausforderung durch:

Qualität

Bedarfsorientierte Entwicklung und Produktion, eingebettet in modernste Qualitätssicherungsmechanismen, sorgen für Erzeugnisse höchster Qualität und langer Nutzbarkeit.

Rücknahmegarantie

Wir sind stolz auf unsere Produkte. Doch geben wir gern zu, dass diese nicht ewig leben. Darum stellen wir, soweit technisch schon möglich und sinnvoll, alle unsere Produkte aus wieder verwendbaren Materialien her. Wir garantieren, dass wir jedes von uns gefertigte Gerät zurücknehmen, die wieder verwendbaren Teile dem Recycling zuführen und den Rest umweltfreundlich entsorgen. Dazu wenden Sie sich an unser Service-Zentrum

Dr. Neuhaus Telekommunikation GmbH
Service-Zentrum
Messestraße 20,
D-18069 Rostock

Bitte helfen Sie uns dabei, die Umwelt zu schützen.

Dr. Neuhaus Telekommunikation GmbH

Inhaltsverzeichnis

1 Einleitung

Produkte

Dieses Handbuch gibt Anweisungen zur Sicherheit und beschreibt die Bedienung und Installation folgender Produkte

	VPN Funktion	HSPA+ / UMTS	E-GPRS	GPRS	CSD
TAINY HMOD-V3-IO	X	X	X	X	X*)
TAINY HMOD-L3-IO	-	X	X	X	X*)
TAINY EMOD-V3-IO	X	-	X	X	X
TAINY EMOD-L3-IO	-	-	X	X	X

*) Nur wenn nicht in einem HSPA+ / UMTS Netz eingebucht

und die zugehörigen Produktvarianten DS (Dual-SIM) und E5 (5-Port-Ethernet-Switch)

Verwendete Produktbezeichnungen

In diesem Handbuch werden Sammelbegriffe für die verschiedenen TAINY-Produktvarianten verwendet:

TAINY xMOD	Sammelbegriff für TAINY HMOD-V3-IO, TAINY HMOD-L3-IO, TAINY EMOD-V3-IO, TAINY EMOD-L3-IO sowie deren Produktvarianten DS und E5
TAINY HMOD	Sammelbegriff für TAINY HMOD-V3-IO, TAINY HMOD-L3-IO sowie deren Produktvarianten DS und E5
TAINY EMOD	Sammelbegriff für TAINY EMOD-V3-IO, TAINY EMOD-L3-IO sowie deren Produktvarianten DS und E5
TAINY xMOD-V3	Sammelbegriff für TAINY HMOD-V3-IO, TAINY EMOD-V3-IO sowie deren Produktvarianten DS und E5
TAINY xMOD-L3	Sammelbegriff für das TAINY HMOD-L3-IO, TAINY EMOD-L3-IO sowie deren Produktvarianten DS und E5

Anwendung

Die TAINY xMOD bieten einen drahtlosen Anschluss zum Internet oder zu einem privaten Netzwerk.

Die TAINY HMOD bieten diesen Anschluss an jedem Ort, an dem ein UMTS-Netz (Universal Mobile Telecommunication System = Mobilfunknetz 3. Generation) oder ein GSM-Netz (Global System for Mobile Communication = Mobilfunknetz) verfügbar ist, das IP-basierte Datendienste bereitstellt. Bei UMTS sind dies HSDPA (High Speed Downlink Packet Access), HSUPA (High Speed Uplink Packet Access) oder der UMTS Data Service und bei GSM sind dies EGPRS (Enhanced General Packet Radio Service = EDGE) oder GPRS (General Packet Radio Service).

HSDPA und HSUPA sind im Folgenden unter dem Begriff HSPA+ zusammengefasst.

Die TAINY EMOD bieten diesen Anschluss an jedem Ort, an dem ein GSM-Netz (Global System for Mobile Communication = Mobilfunknetz) verfügbar ist, das als Dienste EGPRS (Enhanced General Packet Radio Service = EDGE) oder GPRS (General Packet Radio Service) bereitstellt.

Voraussetzung dafür ist eine SIM-Karte eines Mobilfunkbetreibers mit

entsprechend freigeschalteten Diensten.

Die TAINY xMOD-L3 verbinden so eine lokal angeschlossene Applikation oder ganze Netzwerke über drahtlose IP-Verbindungen mit dem Internet. Möglich ist auch die direkte Verbindung mit einem Intranet an dem wiederum die externen Gegenstellen angeschlossen sind.

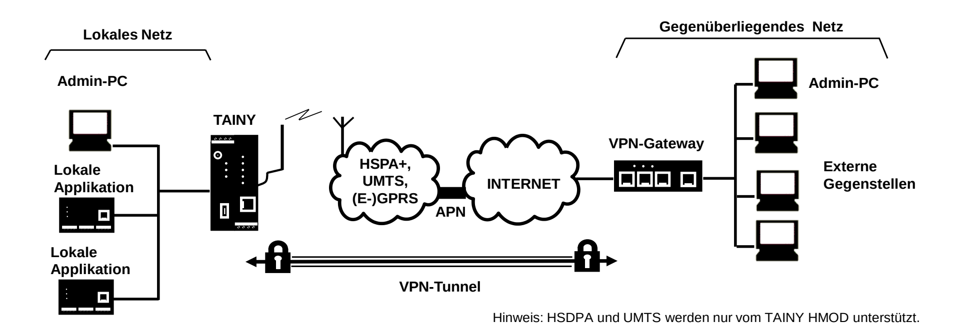
Die TAINY xMOD-V3 können über eine drahtlose IP-Verbindung ein VPN (Virtual Private Network) zwischen einer lokal angeschlossene Applikation/ einem Netzwerk und einem externen Netz aufbauen und diese Verbindung mittels IPsec (Internet Protocol Security) gegen Zugriffe Dritter schützen.

Die Produktvariante DS (Dual-SIM) ermöglicht den alternativen Betrieb mit einer zweiten SIM-Karte, bspw. eines zweiten Betreibers, der die Kommunikation übernimmt, sollte die Verbindung über die erste SIM-Karte gestört sein.

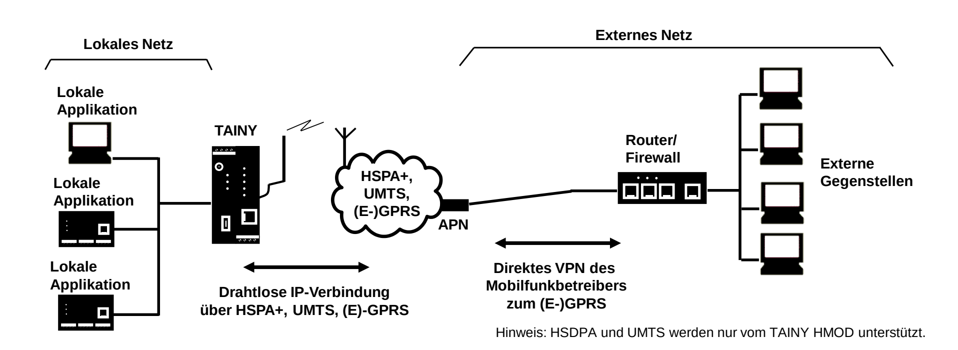
Die Produktvariante E5 (5-Port-Ethernet-Switch) bietet drei zusätzliche Ethernet-Schnittstellen zum Anschluss von weiteren Applikationen an das lokale Netz des TAINY xMOD.

Szenarium 1: Virtual Private Network (VPN) mit Ipsec (Ende zu Ende)

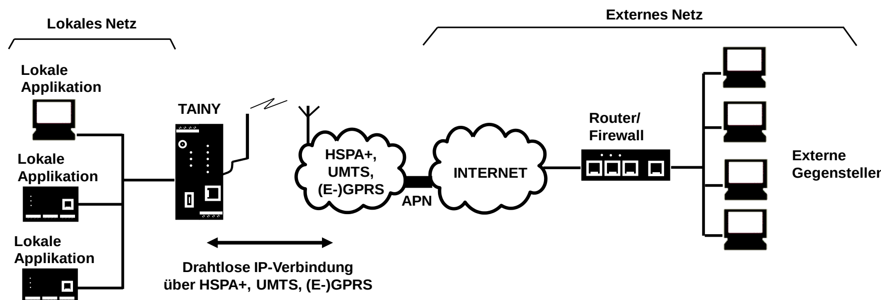
Nur TAINY xMOD-V3



Szenarium 2: Verbindung über HSPA+, UMTS, EGPRS oder GPRS und ein direktes VPN des Mobilfunkbetreibers zum externen Netz:



Szenarium 3: Verbindung über HSPA+, UMTS, EGPRS oder GPRS und das Internet zum externen Netz:



Lokale Applikationen könnten zum Beispiel eine programmierbare Steuerung, eine Maschine mit Ethernet-Schnittstelle zur Fernüberwachung, oder ein Notebook bzw. PC sein. Diese Applikationen benutzen das TAINY xMOD, um Zugriff auf ein externes Netz zu erhalten, so als wenn sie direkt vor Ort an diesem externen Netz angeschlossen wären.

Funktionen

Um die Aufgaben in den beschriebenen Szenarien zu erfüllen, vereinigen die Geräte je nach Ausführung folgende Funktionen:

	TAINY HMOD		TAINY EMOD	
	V3-IO	L3-IO	V3-IO	L3-IO
HSPA+ / UMTS	X	X	-	-
EGPRS / GPRS / CSD	X*)	X*)	X	X
VPN-Funktionen	X	-	X	-
Firewall	X	X	X	X
Konfiguration	X	X	X	X
Weitere Funktionen	X	X	X	X

*) CSD nur, wenn nicht in einem HSPA+ / UMTS Netz eingebucht

Dies gilt auch für entsprechende Geräte der Produktvarianten DS und E5.

Kommunikation

Funkmodem für die flexible Datenkommunikation in UMTS-Netzen

- per HSPA+, UMTS

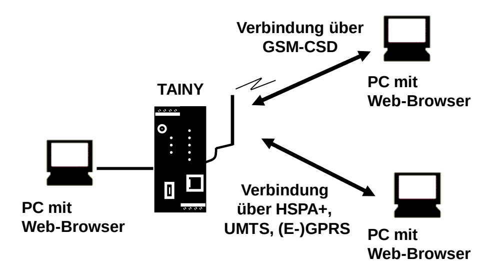
Funkmodem für die flexible Datenkommunikation in GSM-Netzen

- EGPRS, GPRS (und CSD)

Konfiguration

Die Konfiguration des Gerätes erfolgt über eine Web-Oberfläche die sich einfach mit einem Web-Browser anzeigen lässt. Der Zugriff kann über folgende Wege stattfinden:

- die lokale Schnittstelle,
- HSPA+, UMTS, EGPRS, GPRS oder
- CSD (Circuit Switched Data = Datenwählverbindungen) des GSM



Hinweis: HSPA+ und UMTS werden nur vom TAINY HMOD unterstützt.

VPN-Funktionen

TAINY-xMOD-V3-Geräte bieten folgende VPN-Features

- VPN-Router für sichere Datenübertragung über öffentliche Netze
- Protokoll: IPsec (Tunnelmode)
- IPsec-3DES-Verschlüsselung mit 192 Bit
- IPsec-AES-Verschlüsselung mit 128, 192 und 256 Bit
- Paket-Authentisierung: MD5, SHA-1
- Internet Key Exchange (IKE) mit Main und Agressive Mode
- Authentisierung: Pre-Shared Key (PSK), X.509v3 Zertifikate, CA
- NAT-T
- 1-zu-1-NAT
- Dead Peer Detection (DPD)
- Schaltausgang zur Anzeige eines aufgebauten VPN-Tunnels

OpenVPN-Funktionen

- OpenVPN-Client für sichere Datenübertragung über öffentliche Netze
- Authentisierung über Benutzernamen, Passwort und Zertifikat
- LZO-Komprimierung auf dem Datenkanal
- UDP-Paketfragmentierung
- 1-zu-1-NAT
- SNAT

Firewall

Die TAINY xMOD bieten folgende Firewall-Funktionen um das lokale Netz und sich selbst gegen Angriffe von außen zu schützen:

- Stateful Inspection Firewall
- Anti-Spoofing
- Port Forwarding

Weitere Funktionen

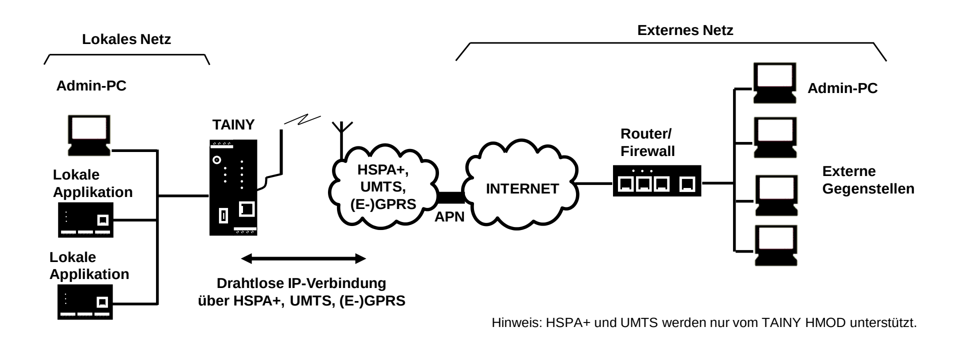
Die TAINY xMOD bieten folgende weitere Funktionen:

- Alternative Anmeldung per TACACS+
- DNS Cache
- DHCP-Server
- NTP
- Remote Logging
- Schalteingang
- Web-Oberfläche zur Konfiguration

- Versand von Alarm-SMS
- Versand von SNMP-Traps
- SMS-Versand aus dem lokalen Netz
- SSH-Konsole zur Konfiguration
- SNMP zur Kontrolle und Konfiguration
- DynDNS-Client
- Datenwählverbindung zur Wartung und Fernkonfiguration
- Volumenüberwachung
- Installationsmodus zur Antennenausrichtung

Begriffe

Häufig verwendete Begriffe in diesem Handbuch werden an dieser Stelle festgelegt:



Lokales Netz	Netzwerk, angeschlossen an der lokalen Schnittstelle der TAINY xMOD. Das lokale Netz enthält mindestens eine lokale Applikation.
Lokale Schnittstellen LAN 0, LAN 1, LAN 2, LAN 3, LAN4 (10/100-Base-T)	Schnittstellen der TAINY xMOD zum Anschluss des lokalen Netzes. Die Schnittstellen sind am Gerät mit LAN 0 und LAN 1 (10/100-Base-T) gekennzeichnet. Es handelt sich um Ethernet-Schnittstellen mit 10Mbit/s oder 100Mbit/s Datenrate (Autosensing MDI/MDIX). Das TAINY xMOD wirkt zwischen beiden Schnittstellen als Switch. Geräte der Produktvariante E5 besitzen darüber hinaus drei weitere, technisch identische Ethernet-Schnittstellen, die mit LAN 2 bis LAN 4 gekennzeichnet sind.
Lokale Applikation	Lokale Applikationen sind Netzwerkkomponenten im lokalen Netz, zum Beispiel eine programmierbare Steuerung, eine Maschine mit Ethernet-Schnittstelle zur Fernüberwachung, ein Notebook bzw. PC oder der Admin-PC.
Admin-PC	Rechner mit Web-Browser (z.B. MS Internet Explorer ab Version 7 oder Mozilla Firefox ab Version 2) angeschlossen an das lokale Netz oder das externe Netz, mit dem die Konfiguration der TAINY xMOD durchgeführt wird. Der Web-Browser muss HTTPS unterstützen. Für die Gerätekonfiguration über SSH wird auf dem Admin-PC ein SSH-Client, wie z.B. putty benötigt.
Externes Netz	Externes Netzwerk, mit dem das TAINY HMOD über HSPA+, UMTS, EGPRS oder GPRS verbunden ist. Externe Netze sind das Internet oder ein privates Intranet. Externes Netzwerk, mit dem das TAINY EMOD über EGPRS oder GPRS verbunden ist. Externe Netze sind das Internet oder ein privates Intranet
Externe Gegenstellen	Externe Gegenstellen sind Netzwerkkomponenten im externen Netz, z.B. Web-Server im Internet, Router im Intranet, ein zentraler Firmenserver, ein Admin-PC und vieles mehr.
(E-)GPRS	EGPRS oder GPRS, je nach Verfügbarkeit der Dienste.

VPN-Gateway	Komponente des externen gegenüberliegenden Netzes, die IPsec unterstützt und kompatibel ist zum TAINY xMOD-V3.
Gegenüberliegendes Netz	Externes Netz, mit dem das TAINY xMOD eine VPN-Verbindung aufbaut.
Mobilfunknetz	Infrastruktur und Technologie zur drahtlosen mobilen Sprach- und Datenkommunikation. Das TAINY HMOD ist für den Einsatz in UMTS-Mobilfunknetzen und GSM-Mobilfunknetzen gebaut, Das TAINY EMOD ist für den Einsatz in EDGE-/GSM-Mobilfunknetzen gebaut.
Datenfunkdienst	Vom verwendeten Mobilfunknetz bereitgestellte Dienste zur Datenübertragung, die vom TAINY xMOD genutzt werden können:

	TAINY HMOD		TAINY EMOD	
	V3-IO	**L3-IO**	**V3-IO**	**L3-IO**
UMTS-Mobilfunknetz	X	X	-	-
HSPA+	X	X	-	-
UMTS data	X	X	-	-
GSM-Mobilfunknetz (mit EDGE)	X	X	X	X
E-GPRS	X	X	X	X
GPRS	X	X	X	X
CSD	X*)	X*)	X	X

*) CSD nur, wenn nicht in einem HSPA+ / UMTS Netz eingebucht

Dies gilt auch für entsprechende Geräte der Produktvarianten DS und E5.

2 Inbetriebnahme

2.1 Schritt für Schritt

Gehen Sie bei der Inbetriebnahme des TAINY xMOD bitte in folgenden Schritten vor:

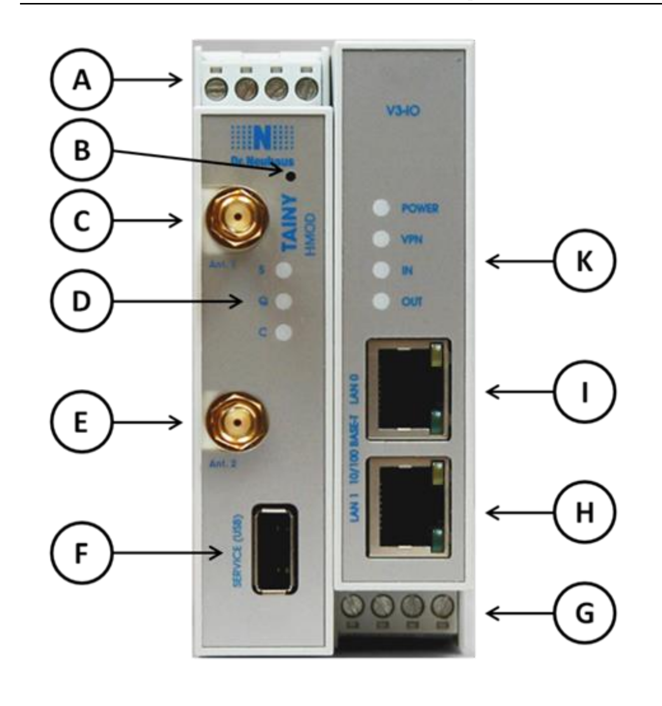
1.	Machen Sie sich bitte zunächst mit den Voraussetzungen für den Betrieb des TAINY xMOD vertraut.	2.2
2.	Lesen Sie bitte sehr sorgfältig die Sicherheitshinweise und weitere Hinweise am Beginn dieses Anwenderhandbuches und befolgen Sie diese bitte unbedingt.	
3.	Machen Sie sich bitte vertraut mit den Bedienelementen, Anschlüssen und Betriebsanzeigen des TAINY xMOD.	2.3 bis 2.7
4.	Schließen Sie einen PC mit Web-Browser (Admin-PC) an eine der lokalen Schnittstellen (10/100 BASE-T) des TAINY xMOD an.	3.3, 3.4
5.	Tragen Sie über die Web-Oberfläche des TAINY xMOD die PIN(s) (Persönliche Identifikations-Nummer(n)) der SIM-Karte(n) ein.	5.1
6.	Trennen Sie das TAINY xMOD wieder von der Versorgungsspannung.	2.7
7.	Legen Sie die SIM-Karte(n) in das Gerät ein.	2.8
8.	Schließen Sie die Antenne(n) an.	2.7
9.	Verbinden Sie das TAINY xMOD mit der Versorgungsspannung.	2.7
10.	Richten Sie das TAINY xMOD nach Ihren Anforderungen ein.	3 bis 12
11.	Schließen Sie Ihre lokale Applikation an.	2.7

2.2 Voraussetzungen für den Betrieb

Um das TAINY xMOD betreiben zu können, müssen die folgenden Informationen vorliegen und die folgenden Voraussetzungen erfüllt sein:

Antenne	Eine Antenne, angepasst auf die Frequenzbänder des von Ihnen gewählten UMTS/GSM-Mobilfunknetzes: 850 MHz, 900 MHz, 1800 MHz, 1900 MHz oder 2100 MHz. Verwenden Sie bitte Antennen aus dem Zubehör zum TAINY xMOD, da diese für den Betrieb mit den Geräten geprüft sind. Siehe Kapitel 2.7.
Spannungsver-sorgung	Eine Spannungsversorgung mit einer Spannung zwischen 12 V_{DC} und 60 V_{DC}, die einen ausreichenden Strom liefern kann (I_{Burst} > 1,26 A). Siehe Kapitel 2.7 und Kapitel 17.
SIM-Karte	Eine SIM-Karte des ausgewählten Mobilfunkbetreibers.
PIN	Die PIN der SIM-Karte
HSPA+ / UMTS/ EGPRS / GPRS Freischaltung	Die SIM-Karte muss von Ihrem Mobilfunk-Netzbetreiber für die Dienste HSPA+, UMTS data (nur TAINY HMOD) und / oder EGPRS oder GPRS freigeschaltet sein. Die Zugangsdaten müssen bekannt sein: - Access Point Name (APN) - Benutzername - Passwort
CSD 9600 bit/s Freischaltung	Die SIM-Karte muss von Ihrem Mobilfunk-Netzbetreiber für den CSD-Dienst freigeschaltet sein, wenn Sie die Fernkonfiguration über Datenwählverbindungen, siehe Kapitel 9.5, nutzen möchten.

2.3 Überblick TAINY xMOD (ohne Produktvariante E5)



A – Anschlussklemmen der Stromversorgung

B – Service-Taster

C – Antennenbuchse 1, Typ SMA

D – Betriebsanzeigen S, Q, C

E - Antennenbuchse 2, Typ SMA (nur TAINY HMOD-x3-IO)

F – Service (USB) – Reserviert für spätere Anwendungen

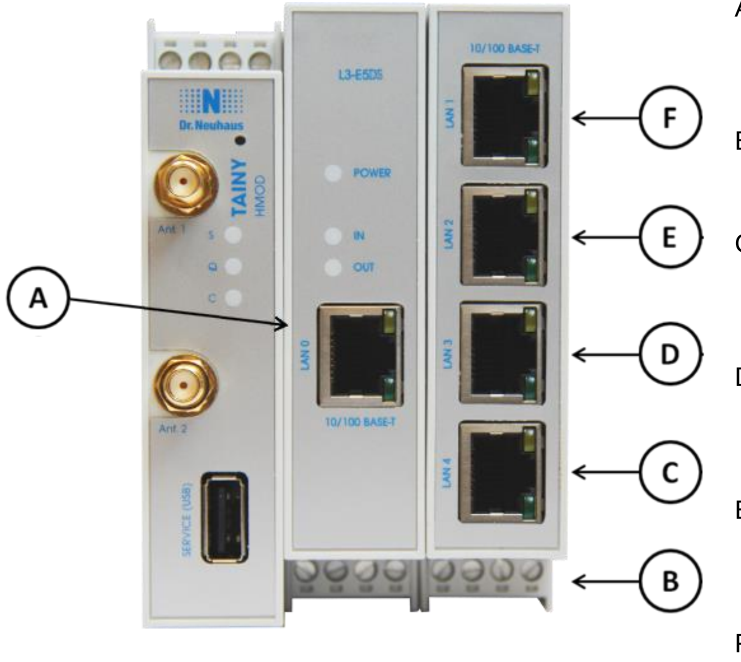
G – Anschlussklemmen des Schalteingangs und Schaltausgangs

H – LAN1 / 10/100-Base-T - RJ45-Buchse zum Anschluss des lokalen Netzes mit integrierten Signalleuchten

I – LAN0 / 10/100-Base-T - RJ45-Buchse zum Anschluss des lokalen Netzes mit integrierten Signalleuchten

K – Betriebsanzeigen
POWER, IN, OUT
VPN (nur TAINY xMOD-V3)

2.4 Überblick TAINY xMOD (Produktvariante E5)



A – LAN0 / 10/100-Base-T - RJ45-Buchse zum Anschluss des lokalen Netzes mit integrierten Signalleuchten

B – Anschlussklemmen – Reserviert für spätere Anwendungen

C – LAN4 / 10/100-Base-T - RJ45-Buchse zum Anschluss des lokalen Netzes mit integrierten Signalleuchten

D – LAN3 / 10/100-Base-T - RJ45-Buchse zum Anschluss des lokalen Netzes mit integrierten Signalleuchten

E - LAN2 / 10/100-Base-T - RJ45-Buchse zum Anschluss des lokalen Netzes mit integrierten Signalleuchten

F – LAN1 / 10/100-Base-T - RJ45-Buchse zum Anschluss des lokalen Netzes mit integrierten Signalleuchten

2.5 Service-Taster



Auf der Frontseite des TAINY xMOD befindet sich ein kleines Loch (siehe Kapitel 2.3, B), hinter dem sich ein Taster befindet. Benutzen Sie einen dünnen Gegenstand, z.B. eine aufgebogene Büroklammer, um den Taster zu drücken

- Wenn Sie den Taster länger als 5 sec drücken, führt das TAINY xMOD einen Neustart durch und lädt dabei die Werkseinstellungen.

2.6 Betriebsanzeigen

Das TAINY xMOD-V3 besitzt 7 Signalleuchten (LEDs), das TAINY xMOD-L3 besitzt 6 Signalleuchten (LEDs) zur Anzeige des Betriebszustands. Dazu kommen noch je 2 integrierte Signalleuchten in den Anschlüssen LAN 0 und LAN 1, bzw. LAN 0 bis LAN 4 bei der Produktvariante E5.

Die 3 Signalleuchten auf der linken Gerätehälfte zeigen den Zustand des Funkmodems an:

TAINY HMOD

Leuchte	Zustand	Bedeutung
S *(Status)*	Langsam blinkend	PIN-Übergabe
	Schnell blinkend	PIN-Fehler / SIM-Fehler
	EIN	PIN-Übergabe erfolgreich
Q *(Quality)*	AUS	Nicht im GSM-Netz eingebucht
	Kurz aufblinkend	Signalstärke schlecht (CSQ < 6)
	Langsam blinkend	Signalstärke mittel (CSQ = 6 - 10)
	EIN mit kurzen Unterbrechungen	Signalstärke gut (CSQ = 11 - 18)
	EIN	Signalstärke sehr gut (CSQ > 18)
C *(Connect)*	AUS	Keine Verbindung
	Schnell blinkend	Service Ruf über CSD aktiv
	Langsam blinkend	EGPRS/GPRS-Verbindung aktiv
	EIN	HSPA+/UMTS-Verbindung aktiv
S, Q, C gemeinsam	schnelles Lauflicht	Booten
	langsames Lauflicht	Update
	synchrones schnelles Blinken	Fehler

TAINY EMOD

Leuchte	Zustand	Bedeutung
S *(Status)*	Langsam blinkend	PIN-Übergabe
	Schnell blinkend	PIN-Fehler / SIM-Fehler
	EIN	PIN-Übergabe erfolgreich
Q *(Quality)*	AUS	Nicht im GSM-Netz eingebucht
	Kurz aufblinkend	Signalstärke schlecht (CSQ < 6)
	Langsam blinkend	Signalstärke mittel (CSQ = 6 - 10)
	EIN mit kurzen Unterbrechungen	Signalstärke gut (CSQ = 11 - 18)
	EIN	Signalstärke sehr gut (CSQ > 18)
C *(Connect)*	AUS	Keine Verbindung
	Schnell blinkend	Service Ruf über CSD aktiv
	EIN mit kurzen Unterbrechungen	GPRS-Verbindung aktiv
	EIN	EGPRS-Verbindung aktiv
S, Q, C gemeinsam	schnelles Lauflicht	Booten
	langsames Lauflicht	Update
	synchrones schnelles Blinken	Fehler

TAINY xMOD-V3

Die 4 Signalleuchten auf der rechten Gerätehälfte (Produktversion IO) bzw. dem mittleren Segment (Produktversion E5) zeigen den Zustand weiterer Gerätefunktionen an:

Leuchte	Zustand	Bedeutung
POWER	EIN	Gerät eingeschaltet, Betriebsspannung liegt an
	AUS	Gerät ausgeschaltet, Betriebsspannung fehlt
VPN	EIN	Mindestens eine VPN-Verbindung aufgebaut
	AUS	Keine VPN-Verbindung aufgebaut
IN	EIN	Schalteingang aktiv
	AUS	Schalteingang nicht aktiv
OUT	EIN	Schaltausgang aktiv
	AUS	Schaltausgang nicht aktiv

TAINY xMOD-L3

Die 3 Signalleuchten auf der rechten Gerätehälfte (Produktversion IO) bzw. dem mittleren Segment (Produktversion E5) zeigen den Zustand weiterer Gerätefunktionen an:

Leuchte	Zustand	Bedeutung
POWER	EIN	Gerät eingeschaltet, Betriebsspannung liegt an
	AUS	Gerät ausgeschaltet, Betriebsspannung fehlt
IN	EIN	Schalteingang aktiv
	AUS	Schalteingang nicht aktiv
OUT	EIN	Reserviert für zukünftige Anwendungen
	AUS	Reserviert für zukünftige Anwendungen

Signalleuchten an den Ethernet-Anschlüssen (2-Port-Version)

Die Signalleuchten an LAN 0 und LAN 1 (Produktversion IO) zeigen den Zustand des entsprechenden Anschlusses an:

Leuchte	Zustand	Bedeutung
LAN 0-1, Grün	AUS	Ethernet-Link nicht erkannt
	AN	Ethernet-Link erkannt
LAN 0-1, Gelb	AUS	Kein Datentransfer
	Blinkend	Datentransfer

Signalleuchten an den Ethernet-Anschlüssen (5-Port-Version)

Die Signalleuchten an LAN 0 bis LAN 4 (Produktversion E5) zeigen den Zustand des entsprechenden Anschlusses an:

Leuchte	Zustand	Bedeutung
LAN 0-4, Grün	AUS AN	Ethernet-Link nicht erkannt Ethernet-Link erkannt
LAN 0, Gelb	AUS Blinkend	Kein Datentransfer Datentransfer
LAN 1-4, Gelb	EIN Blinkend	Kein Datentransfer Datentransfer

2.7 Anschlüsse

LAN 0 - LAN 4 (10/100-Base-T)

An den Anschlüssen LAN 0 und LAN 1 (10/100-Base-T, bei der Produktvariante E5 LAN 0 bis LAN 4) wird das lokale Netz mit den lokalen Applikationen angeschlossen, z.B. eine programmierbare Steuerung, eine Maschine mit Ethernet-Schnittstelle zur Fernüberwachung, ein Notebook bzw. PC.

Das TAINY xMOD wirkt zwischen den verfügbaren Schnittstellen als Switch.

Zum Einrichten des TAINY xMOD schließen Sie hier den Admin-PC mit Web-Browser an.

Die Schnittstellen unterstützen Autonegotiation. Somit wird automatisch erkannt, ob 10 Mbit/s oder 100 Mbit/s Übertragungsgeschwindigkeit auf dem Ethernet genutzt wird.

Die verwendeten Anschlusskabel müssen einen RJ45-Stecker haben. Sie können Cross-over oder Eins-zu-Eins verdrahtet sein (MDI/MDIX).

Service (USB)

Diese Schnittstelle ist beim TAINY xMOD ohne Funktion und reserviert für spätere Anwendungen. Bitte schließen Sie hier keine Geräte an. Der Betrieb des TAINY xMOD könnte gestört werden.

SMA Antennen-Buchse(n)

Das TAINY HMOD hat zwei Antennenbuchsen vom Typ SMA zum Anschluss von Antennen, das TAINY EMOD hat eine Antennenbuchse vom Typ SMA zum Anschluss einer Antenne. Achten Sie darauf, dass sowohl beim TAINY HMOD als auch beim TAINY EMOD im Betrieb immer mindestens eine Antenne angeschlossen ist. Beim TAINY HMOD muss diese Antenne am Anschluss Ant. 1 angeschlossen werden.

Am TAINY HMOD kann zur Verbesserung der Empfangseigenschaften eine zweite Antenne am Anschluss Ant. 2 angeschlossen werden.

Die verwendeten Antennen sollen eine Impedanz von ca. 50 Ohm haben. Sie müssen abgestimmt sein für GSM 900MHz und DCS 1800MHz oder GSM 850 MHz und PCS 1900 MHz, oder für UMTS 2100 MHz je nachdem, welche Frequenzbänder ihr UMTS/GSM-Mobilfunkbetreiber verwendet. In Europa und China werden GSM 900MHz, DCS 1800MHz und UMTS 2100MHz verwendet, in den USA verwendet man GSM 850

MHz und PCS 1900 MHz (auch für UMTS). Bitte erkundigen Sie sich bei Ihrem Netzbetreiber.

Die Anpassung (VSWR) der Antenne muss 1:2,5 oder besser sein.

Achtung:

Verwenden Sie bitte nur Antennen aus dem Zubehörprogramm für das TAINY xMOD. Diese Antennen sind von uns geprüft und gewährleisten die beschriebenen Produkteigenschaften.

Bei der Installation der Antenne ist auf eine ausreichend gute Signalqualität zu achten (CSQ > 11). Nutzen Sie die Signalleuchten des TAINY xMOD, die Ihnen die Signalqualität anzeigen oder die Ausgabe des *Netzwerkstatus*, siehe Kapitel 5.6. Achten Sie bitte darauf, dass sich keine großen metallischen Gegenstände (z.B. Stahlbeton) in der Nähe der Antenne befinden.

Die zweite Antenne des TAINY HMOD sollte etwa 30 bis 100 cm entfernt von der ersten Antenne positioniert werden.

Bitte beachten Sie die Montage- und Gebrauchsanleitung der verwendeten Antenne

---

Warnung:

Bei Außenmontage der Antenne muss die Antenne zwecks Blitzschutzes geerdet werden. Diese Arbeiten müssen von einer qualifizierten Fachkraft durchgeführt werden. Die Sicherheitshinweise am Beginn dieser Anleitung sind zu beachten.

Schraubklemmen

Versorgung

24V 0V

Schalteingang/Schaltausgang



24V / 0V Versorgungs-Spannung

Das TAINY xMOD arbeitet mit einer Gleichspannung von 12-60 V DC, nominell 24 V DC. Diese Versorgungsspannung wird an die Schraubklemmen der linken Gerätehälfte angeschlossen.

Die Stromaufnahme beträgt etwa 450mA bei 12V und 100mA bei 60V (I_{Burst} > 1,26 A).

Warnung:

Das Netzteil des TAINY xMOD ist nicht potentialgetrennt.

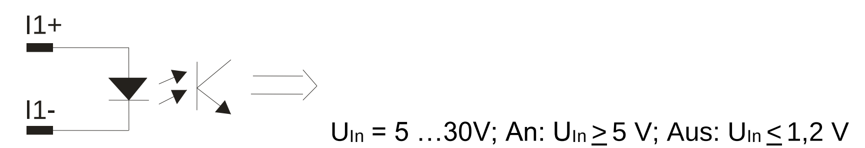
Beachten Sie bitte die Sicherheitshinweise am Anfang dieses Handbuchs.

Hinweis

Achten Sie bitte auf eine ausreichende Dimensionierung der Versorgungsquelle. Eine zu schwache Versorgung kann zu einem instabilen Betrieb führen.

Schalteingang I1+/ I1-

Das TAINY xMOD hat einen Schalteingang. Der Schalteingang hat seine Anschlüsse an den Schraubklemmen der rechten Gerätehälfte. Die Klemmen sind mit I1+/I1- bezeichnet.



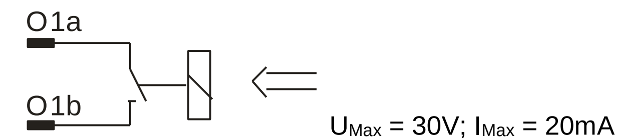
Zur Funktion des Schalteingangs siehe auch Kapitel 10.6.

Warnung:

Der Schalteingang ist gegenüber den anderen Anschlüssen des TAINY xMOD galvanisch getrennt. Verbindet die am TAINY xMOD angeschlossene Installation ein Signal des Schalteingangs galvanisch mit der Versorgungsspannung, darf zwischen jedem Signal des Schalteingangs und jedem Anschluss der Versorgungsspannung des TAINY xMOD die Spannung jeweils 60V nicht überschreiten.

Schaltausgang O1a/ O1b

Das TAINY xMOD-V3 hat einen Schaltausgang. Der Schaltausgang hat seine Anschlüsse an den Schraubklemmen der rechten Gerätehälfte, bzw. des mittleren Segments bei der Produktvariante E5. Die Klemmen sind mit O1a/O1b bezeichnet.



Der Schaltausgang ist aktiv (Schalter geschlossen), wenn mindestens eine VPN-Verbindung aufgebaut ist.

Der Schaltausgang ist nicht aktiv (Schalter offen), wenn keine VPN-Verbindung aufgebaut ist.

Warnung:

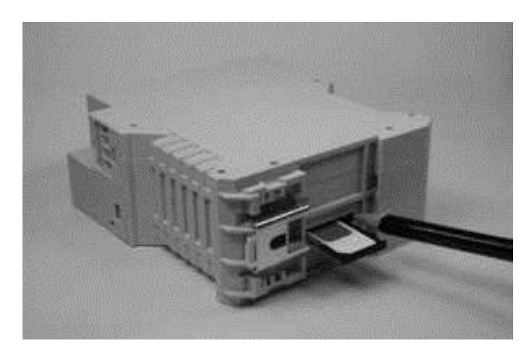
Der Schaltausgang ist gegenüber den anderen Anschlüssen des TAINY xMOD galvanisch getrennt. Verbindet die am TAINY xMOD angeschlossene Installation ein Signal des Schaltausgangs galvanisch mit der Versorgungsspannung, darf zwischen jedem Signal des Schaltausgangs und jedem Anschluss der Versorgungsspannung des TAINY xMOD die Spannung jeweils 60V nicht überschreiten.

Zusatzklemmblock der Produktvariante E5

Geräte der Produktvariante E5 besitzen im rechten Segment einen weiteren 4-poligen Schraubklemmblock.

Diese Schnittstelle ist beim TAINY xMOD ohne Funktion und reserviert für spätere Anwendungen. Bitte schließen Sie hier keine Geräte an. Der Betrieb des TAINY xMOD könnte gestört werden.

2.8 Die SIM-Karte einlegen



Achtung:

Bevor Sie die SIM-Karte einlegen, tragen Sie bitte im TAINY xMOD über die Web-Oberfläche die PIN der SIM-Karte ein. Siehe Kapitel 5.1.

1. Nachdem Sie die PIN der SIM-Karte eingetragen haben, trennen Sie bitte das TAINY xMOD vollständig von der Versorgungsspannung.
2. Die Schublade für die SIM-Karte befindet sich auf der Geräterückseite. In der Gehäuseöffnung befindet sich direkt neben der Schublade für die SIM-Karte ein kleiner gelber Taster. Drücken Sie auf diesen Taster mit einem spitzen Gegenstand, z.B. einem Bleistift.

   Bei Druck auf den Taster, kommt die SIM-Karten-Schublade aus dem Gehäuse.
3. Legen Sie die SIM-Karte so in die Schublade, dass ihre vergoldeten Kontakte sichtbar bleiben.
4. Schieben Sie dann bitte die Schublade mit der SIM-Karte vollständig in das Gehäuse.



Achtung!

Legen Sie die SIM-Karte auf keinen Fall im Betrieb ein oder entfernen Sie sie. Die SIM-Karte und das TAINY xMOD könnten beschädigt werden.

NUR Geräte der Produktvariante DS



Geräte der Produktvariante DS besitzen eine zweite Öffnung für eine weitere SIM-Karten-Schublade auf der Geräterückseite. Bitte beachten Sie auch beim Einlegen der zweiten SIM-Karte die oben beschriebenen Hinweise.

3 Konfiguration

3.1 Übersicht

Die Konfiguration der Router- und Firewall-Funktionen erfolgt lokal oder aus der Ferne über die web-basierte Administrations-Oberfläche des TAINY xMOD. Für das TAINY xMOD-V3 kann zusätzlich eine Konfiguration der VPN-Funktion erfolgen.

Fernkonfiguration

Eine Fernkonfiguration über HTTPS- oder CSD-Zugang ist nur möglich, sofern das TAINY xMOD für Fernzugriffe konfiguriert ist. Sie gehen in diesem Fall genauso vor, wie in Kapitel 8 beschrieben.

Konfiguration über die lokale Schnittstelle

Die Voraussetzungen für die Erstkonfiguration über die lokale Schnittstelle sind:

- Der Rechner (Admin-PC), mit dem Sie die Konfiguration vornehmen, muss entweder
  - direkt an der Ethernet-Buchse des TAINY xMOD per Netzwerkkabel angeschlossen sein

  oder

  - über das lokale Netz direkten Zugriff auf das TAINY xMOD haben.
- Der Netzwerkadapter des Rechners (Admin-PC), mit dem Sie die Konfiguration vornehmen, muss folgende TCP/IP Konfiguration haben:

  IP-Adresse: **192.168.1.2**

  Subnetzmaske: **255.255.255.0**

  Statt der IP-Adresse **192.168.1.2** können Sie auch andere IP-Adressen aus dem **Bereich 192.168.1.x** verwenden, aber nicht 192.168.1.1, 192.168.1.0 und 192.168.1.255.
- Wenn Sie mit dem Admin-PC über das TAINY xMOD auch auf das externe Netz zugreifen möchten, sind zusätzlich folgende Einstellungen erforderlich:

  Standardgateway: **192.168.1.1**

  Bevorzugter DNS-Server: **Adresse des Domain Name Servers**

3.2 Erlaubte Zeichen bei Benutzernamen, Passwörtern und weiteren Eingaben

Erlaubte Zeichen

Bei Eingaben von Benutzernamen, Passwörtern, Host-Namen, APN und PIN sind folgende darstellbare ASCII-Zeichen erlaubt:

Benutzernamen und Passwörter	@ ~ % $, * ' = ! + - \ / ? ( ) { } . : ; [ ] _ | 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z Bei den Zugangsparametern für UMTS bzw. EGPRS und GPRS (Siehe Kap. 5.1) ist auch # als Zeichen erlaubt.
Host-Namen und APN	. - 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z
PIN	Für PIN-Eingaben sind nur numerische Zeichen erlaubt: 0 1 2 3 4 5 6 7 8 9 Einige Parameter erlauben weitere Sonderzeichen.

3.3 TCP/IP Konfiguration des Netzwerkadapters unter Windows XP

Windows Verbinden mit…

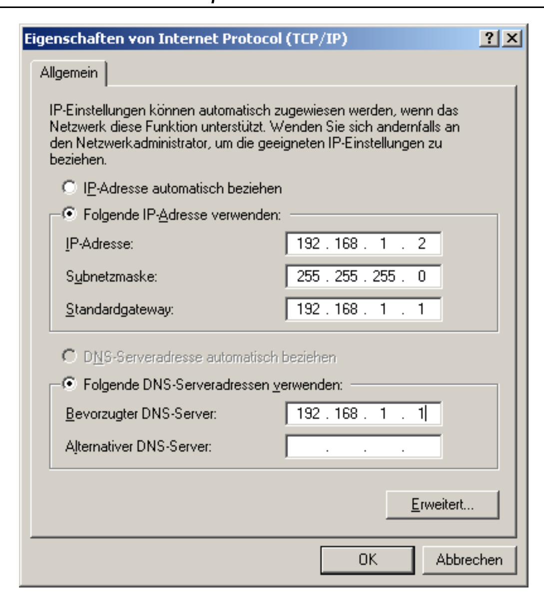
Klicken Sie *Start, Verbinden mit ..., Alle Verbindungen anzeigen…*

Klicken Sie dann auf *LAN-Verbindung.* Wählen sie im Dialogfeld *Eigenschaften von LAN-Verbindung* die Registerkarte *Allgemein* und markieren Sie dort den Eintrag *Internetprotokoll (TCP/IP).* Öffnen Sie *Eigenschaften* durch klicken auf diese Schaltfläche.

Es erscheint das Fenster *Eigenschaften von Internetprotokoll TCP/IP* (siehe Abbildung unten).

Hinweis

Der Weg der zum Dialogfeld *Eigenschaften von LAN-Verbindung* führt hängt von Ihren Windows Einstellungen ab. Können Sie das Dialogfeld nicht finden, suchen Sie bitte in der Windows-Hilfe nach *LAN-Verbindung* oder *Eigenschaften von Internetprotokoll TCP/IP*.



Geben Sie folgende Werte ein, um die Web-Oberfläche des TAINY xMOD zu erreichen:

IP-Adresse: **192.168.1.2**

Subnetzmaske: **255.255.255.0**

Geben Sie zusätzlich folgende Werte ein, wenn Sie mit dem Admin-PC über das TAINY xMOD auf das externe Netz zugreifen wollen:

Standardgateway: **192.168.1.1**

Bevorzugter DNS-Server: **Adresse des Domain Name Servers**

Bevorzugter DNS-Server

Wenn Sie Adressen über einen Domain-Namen aufrufen (z. B. www.neuhaus.de), dann muss auf einem Domain Name Server (DNS) nachgeschlagen werden, welche IP-Adresse sich hinter dem Namen verbirgt. Als Domain Name Server können Sie festlegen:

- DNS-Adresse des Netzbetreibers

  oder

- Lokale IP-Adresse des TAINY xMOD, sofern dieses zum Auflösen von Host-Namen in IP-Adressen konfiguriert ist (siehe Kapitel 4.4). Dies ist die **Werkseinstellung**.

Um den Domain Name Server in der TCP/IP-Konfiguration Ihres Netzwerkadapters festzulegen, gehen Sie wie oben beschrieben vor.

3.4 Konfigurations-Verbindung herstellen

Web-Browser einrichten

Gehen Sie wie folgt vor:

1. Starten Sie einen Web-Browser (z.B. MS Internet Explorer ab Version 7 oder Mozilla Firefox ab Version 2); der Web-Browser muss SSL (d. h. HTTPS) unterstützen.

2. Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt.

   Im MS Internet Explorer 7 nehmen Sie diese Einstellung wie folgt vor: Menü *Extras, Internetoptionen...*, Registerkarte *Verbindungen*: Die Option *Keine Verbindung wählen* muss aktiviert sein.

Startseite des TAINY xMOD aufrufen

3. In der Adresszeile des Browsers geben Sie die Adresse TAINY xMOD vollständig ein. Gemäß Werkseinstellung lautet diese:

   https://192.168.1.1

   Folge: Es erscheint ein Sicherheitshinweis. Beim Internet Explorer 7 zum Beispiel dieser:

Sicherheitshinweis bestätigen



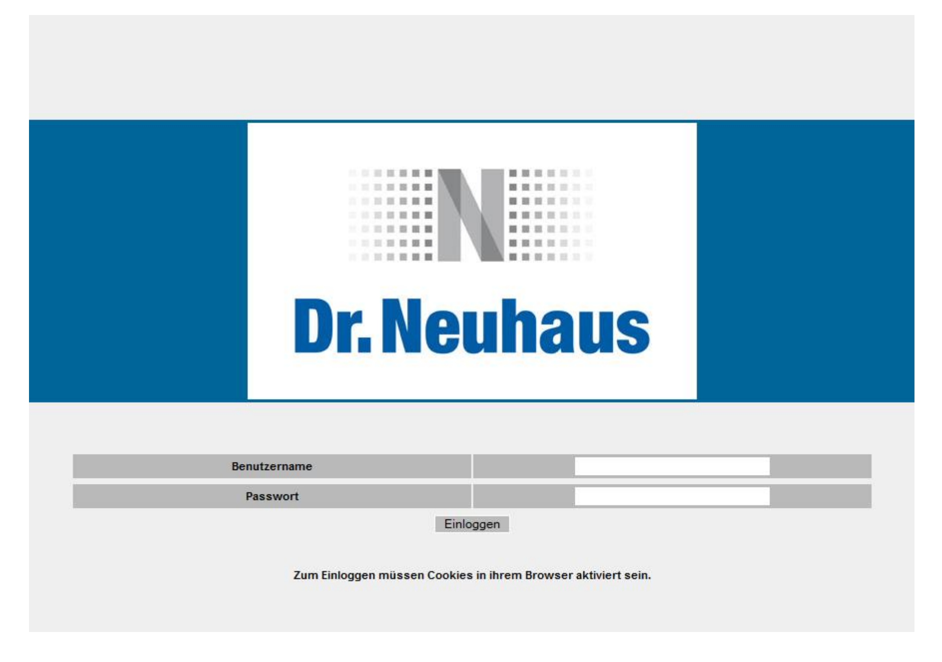
4. Quittieren Sie den entsprechenden Sicherheitshinweis mit „Laden dieser Webseite fortsetzen …“

Hinweis

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbst unterzeichneten Zertifikat ausgeliefert. Bei Zertifikaten mit Unterschriften, die dem Betriebssystem nicht bekannt sind, erfolgt ein Sicherheitshinweis. Sie können sich das Zertifikat anzeigen lassen.
Aus dem Zertifikat muss erkenntlich sein, dass es für Dr. Neuhaus Telekommunikation GmbH ausgestellt wurde. Die Web-Oberfläche wird über eine IP-Adresse adressiert und nicht über einen Namen, daher stimmt der im Sicherheitszertifikat angegebene Name nicht mit dem im Zertifikat überein.

5. Sie werden aufgefordert, den Benutzernamen und das Passwort (Kennwort) anzugeben:

Benutzername und Passwort eingeben



Die werkseitige Voreinstellung lautet:

Benutzername: **root**

Kennwort: **root**

Hinweis

Sie sollten auf jeden Fall das Passwort (Kennwort) ändern. Die werkseitige Voreinstellung ist allgemein bekannt und ist kein ausreichender Schutz. Im Kapitel 3.9 ist beschrieben, wie das Passwort geändert werden kann.

Hinweis

Damit Sie sich erfolgreich am TAINY xMOD anmelden können, müssen Sie in Ihrem Browser Cookies aktivieren.

Hinweis

Ist im TAINY xMOD bereits die Authentifizierung über TACACS+ aktiviert, zeigt der Anmeldebildschirm zusätzlich ein Auswahlmenü, in dem die Anmeldung über TACACS+ oder die normale, lokale Anmeldung gewählt werden kann. Im Folgenden wird zunächst die lokale Anmeldung beschrieben, die bei Erstinbetriebnahme des Geräts verwendet wird. Für weitere Informationen über die Anmeldung per TACACS+ siehe Kapitel 9.2.

Die Startseite wird angezeigt

Nach Eingabe von Benutzernamen und Passwort erscheint im Web-Browser die Startseite des TAINY xMOD mit einem Überblick über den Betriebszustand, siehe Kapitel 3.5.

Die Startseite wird nicht angezeigt

Sollte auch nach wiederholtem Versuch der Browser melden, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Überprüfen Sie die Hardware-Verbindung. Dazu bei einem Windows-Rechner über die DOS-Eingabeaufforderung (Menü *Start, Programme, Zubehör, Eingabeaufforderung*) folgenden Befehl eingeben:

  ping 192.168.1.1

  Wenn innerhalb der vorgegebenen Zeitspanne die Meldung über den Rück-Empfang der 4 ausgesendeten Pakete nicht erscheint, überprüfen Sie bitte das Kabel, die Anschlüsse und die Netzwerkkarte.

- Achten Sie darauf, dass der Browser keinen Proxy Server verwendet. Im MS Internet Explorer (Version 7.0) nehmen Sie diese Einstellung wie folgt vor: Menü *Extras, Internetoptionen...*, Registerkarte *Verbindungen*: Unter *LAN-Einstellungen* auf die Schaltfläche *Einstellungen...* klicken, im Dialogfeld *Einstellungen für lokales Netzwerk (LAN)* dafür sorgen, dass unter *Proxyserver* der Eintrag *Proxyserver für LAN verwenden* nicht aktiviert ist.

- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.
  Unter Windows Menü *Start, Verbinden mit ..., Systemsteuerung, Alle Verbindungen anzeigen* unter LAN oder Höchstgeschwindigkeits-Internet die betreffende Verbindung mit der rechten Maustaste klicken und im Kontextmenü *Deaktivieren* wählen.

- Geben Sie die Adresse des TAINY xMOD mit Slash ein:

  https://192.168.1.1/

3.5 Konfigurations-Verbindung trennen (Abmeldung vom TAINY xMOD)

Logout

Durch Klicken auf den Menüpunkt *Logout* können Sie sich manuell vom TAINY xMOD abmelden. Die Konfigurations-Verbindung wird dabei getrennt und die Weboberfläche wechselt zurück zum Anmeldebildschirm.



Soll die Konfigurationsverbindung wieder aufgebaut werden, müssen Benutzername und Passwort erneut eingegeben werden.

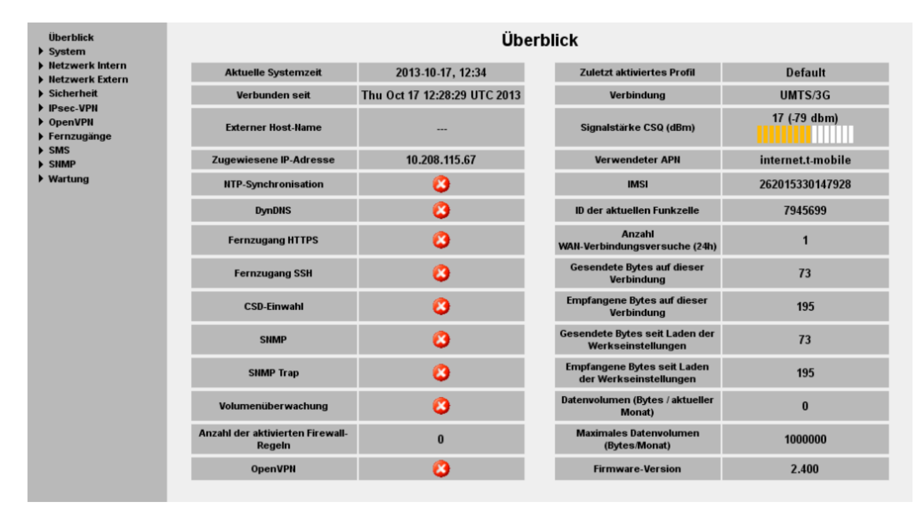
Gehen Sie hierzu wie in Kapitel 3.4 beschrieben vor.

Hinweis

Findet 15 min lang kein Datentransfer über die Konfigurations-Verbindung statt, trennt das Gerät die Verbindung automatisch. Beim nächsten Zugriff auf eine Webseite wechselt es zurück zum Anmeldebildschirm. Soll die Konfigurationsverbindung wieder aufgebaut werden, gehen Sie bitte wie im Kapitel 3.4 beschrieben vor.

3.6 System Status (Startseite)

Überblick



Nach Aufrufen der Web-Oberfläche des TAINY xMOD und der Eingabe von Benutzernamen und Passwort erscheint ein Überblick über den aktuellen Betriebszustand des Gerätes.

Hinweis

Benutzen Sie die Funktion *Aktualisieren* des Web-Browsers um die angezeigten Werte auf den aktuellen Stand zu bringen.

Zuletzt aktiviertes Profil

Zeigt den Namen des zuletzt aktivierten Profils an.

Hinweis

Der Inhalt dieses Profils muss nicht mit den aktuell eingestellten Werten des TAINY xMOD übereinstimmen, sofern Änderungen, die nach dem Laden des Profils durchgeführt wurden, nur in der aktuellen Konfiguration, aber nicht im hinterlegten Profil abgespeichert werden.

Aktuelle Systemzeit

Zeigt die aktuelle Systemzeit des TAINY xMOD an, im Format:

Jahr – Monat – Tag, Stunden – Minuten

Verbunden seit

Zeigt an, seit wann die aktuelle Verbindung zum Datenfunkdienst besteht.

Externer Host-Name

Zeigt den Host-Namen (z.B. tainy.mydns.org) des TAINY xMOD an, wenn ein DynDNS-Dienst verwendet wird.

Zugewiesene IP-Adresse

Zeigt die IP-Adresse an, unter der das TAINY xMOD über den Datenfunkdienst zu erreichen ist. Diese IP-Adresse wird dem TAINY xMOD vom Datenfunkdienst zugewiesen.

Verbindung

Zeigt an ob, und welche Funkverbindung besteht.

Bei TAINY HMOD:

- UMTS-Verbindung (IP-Verbindung über HSPA+, UMTS data)
- GPRS/EDGE-Verbindung (IP-Verbindung über EGPRS oder GPRS)
- CSD-Verbindung (Service-Verbindung über CSD)

Bei TAINY EMOD:

- EDGE-Verbindung (IP-Verbindung über EGPRS)
- GPRS-Vebindung (IP-Verbindung über GPRS)
- CSD-Verbindung (Service-Verbindung über CSD)

Bei Verbindungsproblemen werden an dieser Stelle entsprechende Hinweise angezeigt.

Hinweis

Es kann vorkommen, dass eine Funkverbindung und auch eine zugewiesene IP-Adresse angezeigt werden, die Verbindungsqualität aber dennoch nicht ausreicht um Daten zu übertragen. Aus diesem Grunde empfehlen wir, die aktive Verbindungsüberwachung (siehe Kapitel 5.2) zu nutzen.

Signalstärke CSQ (dBm)

Gibt die Stärke des GSM-Signals als CSQ-Wert und (in Klammern) als RSSI-Wert in dBm an.

- CSQ = 0: Keine Verbindung zum Funknetz
- CSQ < 6: Signalstärke schlecht
- CSQ = 6..10: Signalstärke mittel
- CSQ = 11..18: Signalstärke gut
- CSQ > 18: Signalstärke sehr gut

Verwendeter APN

Zeigt den verwendeten APN (= Access Point Name) des Datenfunkdienstes an.

IMSI

Zeigt die Teilnehmerkennung an, die auf der verwendeten SIM-Karte gespeichert ist.

Anhand der IMSI (= International Mobile Subscriber Identity) erkennt der GSM-Netzbetreiber die Berechtigungen und vereinbarten Dienste der SIM-Karte.

NTP-Synchronisation

Zeigt an, ob die NTP-Synchronisation aktiviert ist.

NTP-Synchronisation aktiviert.

NTP-Synchronisation nicht aktiviert

DynDNS

Zeigt an, ob ein DynDNS-Dienst aktiviert ist.

DynDNS-Dienst aktiviert.

DynDNS-Dienst nicht aktiviert

Fernzugang HTTPS

Zeigt an, ob Zugriffe auf die Web-Oberfläche des TAINY xMOD aus der Ferne über den Datenfunkdienst erlaubt sind (siehe Kapitel 9.1).

Der Zugriff per HTTPS ist erlaubt.

Der Zugriff per HTTPS ist nicht erlaubt.

Fernzugang SSH

Zeigt an, ob Zugriffe auf die SSH-Konsole des TAINY xMOD aus der Ferne über den Datenfunkdienst erlaubt sind (siehe Kapitel 9.4).

Der Zugriff per SSH ist erlaubt.

Der Zugriff per SSH ist nicht erlaubt.

CSD-Einwahl

Zeigt an, ob CSD-Serviceanrufe aus der Ferne erlaubt sind.

CSD-Serviceanrufe sind möglich.

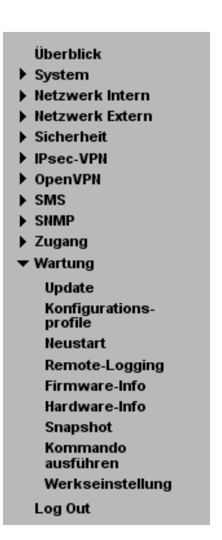
	✗ CSD-Serviceanrufe sind nicht möglich.
SNMP	Zeigt an, ob das Setzen und Lesen von Parametern per SNMP freigegeben ist (siehe Kapitel 12.1): ✓ Setzen/Lesen von Parametern per SNMP ist erlaubt. ✗ Setzen/Lesen von Parametern per SNMP ist nicht erlaubt.
SNMP-Trap	Zeigt an, ob das Versenden von SNMP-Benachrichtigungen (SNMP-Traps) freigegeben ist (siehe Kapitel 12.2): ✓ Versand von SNMP-Benachrichtungen aktiviert. ✗ SNMP-Benachrichtungen nicht aktiviert.
Volumenüberwachung	Zeigt an, ob die Volumenüberwachung eingeschaltet ist (siehe Kapitel 5.7): ✓ Volumenüberwachung ist aktiviert. ✗ Volumenüberwachung ist nicht aktiviert.
ID der aktuellen Funkzelle	Zeigt die Kennung der Mobilfunk-Basisstation an, mit der das TAINY xMOD derzeit verbunden ist.
Anzahl WAN-Verbindungsversuche (24h)	Zeigt die Anzahl der Anmeldeversuche des TAINY xMOD am APN seit 0:00 Uhr (Systemzeit) an. Der Wert 0 zeigt an, dass kein erneuter Anmeldeversuch stattgefunden hat.
Gesendete Bytes / Empfangene Bytes auf dieser Verbindung	Zeigt die Anzahl der Bytes an, die während der bestehenden Verbindung über den Datenfunkdienst gesendet bzw. empfangen worden sind. Die Zähler werden bei Aufbau einer neuen Verbindung zurückgesetzt. **Hinweis** Diese Zahlen dienen nur als Anhaltspunkt für das Datenvolumen und können von der Abrechnung des Netzbetreibers abweichen.
Gesendete Bytes / Empfangene Bytes seit Laden der Werkseinstellungen	Zeigt die Anzahl der Bytes an, die seit dem letzten Laden der Werkseinstellung über den Datenfunkdienst gesendet bzw. empfangen worden sind. Die Zähler werden bei Laden der Werkseinstellung zurückgesetzt.
Datenvolumen (Bytes / aktueller Monat)	Zeigt die Anzahl der gesendeten und empfangenen Bytes seit Monatsbeginn (Systemzeit) an. **Hinweis** Diese Zahlen dienen nur als Anhaltspunkt für das Datenvolumen und können von der Abrechnung des GSM-Netzbetreibers deutlich abweichen. Die NTP-Synchronisation muss aktiviert sein.
Maximales Daten-volumen (Bytes/Monat)	Zeigt die eingestellte Warnschwelle des Datenvolumens an, bei der das TAINY xMOD eine Benachrichtigung versendet.
Anzahl der aktivierten Firewall-Regeln	Zeigt an wie viele Firewall-Regeln aktiviert sind.
Firmware-Version	Zeigt die Versionsnummer der Software des TAINY xMOD an.

3.7 Konfiguration vornehmen

Zur Konfiguration gehen Sie wie folgt vor:

Konfiguration durchführen

1. Per Menü den gewünschten Einstellbereich aufrufen
2. auf der betreffenden Seite die gewünschten Einträge machen oder mit **Zurücksetzen** die aktuelle, nicht gespeicherte Eingabe wieder löschen.
3. mit **Speichern** bestätigen, so dass die Einstellungen vom Gerät übernommen werden.



NUR TAINY xMOD-V3

Hinweis zum Funktionsumfang

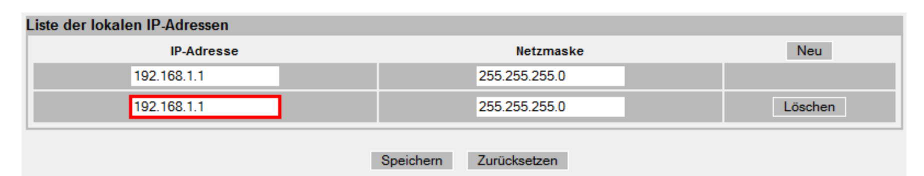
Der Menüpunkt IPsec-VPN findet sich nur bei TAINY xMOD-V3-Geräten.

➲ Je nachdem, wie Sie das TAINY xMOD konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

➲ Tragen Sie bei der Eingabe von IP-Adressen, die IP-Adress-Teilnummern immer ohne führende Nullen ein, z.B.: 192.168.0.8.

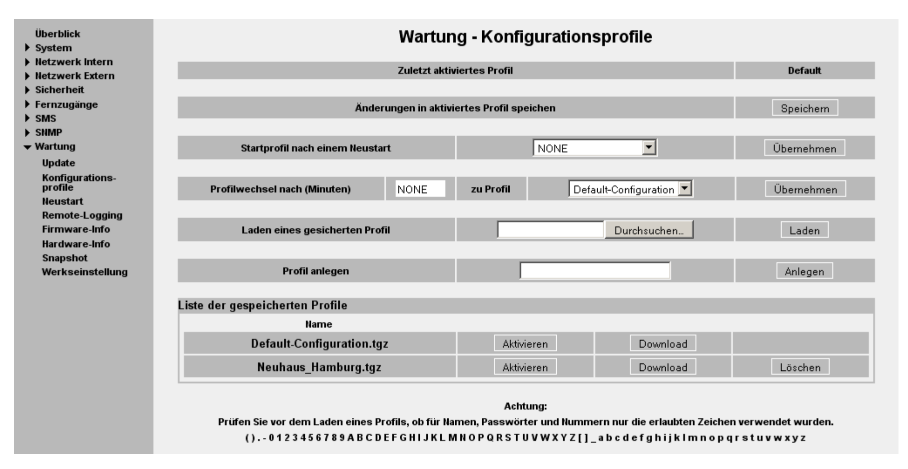
Fehleingaben

Das TAINY xMOD prüft Ihre Eingaben. Grobe Fehler werden beim Speichern erkannt, das betroffene Eingabefeld wird markiert und der eingetragene Wert wird auf den Default-Wert zurückgesetzt.



3.8 Konfigurationsprofile

Wartung > Konfigurations-profile



Funktion

Die Einstellungen des TAINY xMOD können in Konfigurationsprofilen (Dateien) gespeichert und jederzeit neu geladen werden.

Zuletzt aktiviertes Profil	Zeigt den Namen des zuletzt im TAINY xMOD aktivierten Konfigurationsprofils an. Wurde seit Inbetriebnahme noch kein Konfigurationsprofil aktiviert oder das Gerät anderweitig wieder in den Werkszustand zurückversetzt (siehe 3.11) wird hier *Default* angegeben.
Änderungen in aktiviertes Profil speichern	Das Speichern von Änderungen direkt auf den entsprechenden Webseiten wirkt sich nur auf die aktuell aktive Konfiguration des Geräts aus, nicht aber auf das unter *Zuletzt aktiviertes Profil* angegebene Konfigurationsprofil. Sobald ein Konfigurationsprofil geladen wird, werden diese Änderungen verworfen. Mit der Schaltfläche *Änderungen in aktiviertes Profil speichern* können Änderungen, die nach dem letzten Aktivieren eines Profils durchgeführt wurden, in das unter *Zuletzt aktiviertes Profil* angegebene Konfigurationsprofil gespeichert werden.
Startprofil nach einem Neustart	Hier kann ein im Gerät hinterlegtes Konfigurationsprofil ausgewählt werden, das nach einem Neustart aktiviert werden soll. Ist *NONE* ausgewählt, startet das Gerät mit der Konfiguration, die vor dem Neustart aktiv war.
Profilwechsel nach (Minuten)	Profilwechsel können zeitgesteuert durchgeführt werden. Die Parameter haben folgende Bedeutung *Profilwechsel nach (Minuten)*: Geben Sie hier die Zeitspanne in Minuten an, nach deren Ablauf ein Profilwechsel durchgeführt werden soll *zu Profil*: Wählen Sie hier ein im Gerät hinterlegtes Konfigurationsprofil aus, das durch einen zeitgesteuerten Profilwechsel aktiviert werden soll.
Laden eines gesicherten Profils	Lädt ein zuvor erstelltes und auf den Admin-PC gespeichertes Konfigurationsprofil in das TAINY xMOD. Dateien mit Konfigurationsprofilen haben die Dateiendung *.tgz. Mit *Durchsuchen* können Sie auf dem Admin-PC nach Konfigurationsprofilen suchen, mit *Laden* übertragen Sie das Konfigurationsprofil in das TAINY xMOD. Es wird dann in der Tabelle der gespeicherten Konfigurationsprofile angezeigt.
Profil anlegen	Speichert die aktuellen Einstellungen des TAINY xMOD in einem Konfigurationsprofil. Geben Sie zunächst einen Namen für das Profil in dem Eingabefeld ein. Für den Namen dürfen folgende Zeichen verwendet werden: ( ) . - 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ ] _ a b c d e f g h i j k l m n o p q r s t u v w x y z Mit *Anlegen* werden die Einstellungen in einem Profil mit diesem Namen gespeichert und dann in der Liste der gespeicherten Profile angezeigt.
Liste der gespeicherten Profile	Die Liste der gespeicherten Profile zeigt alle Konfigurationsprofile an, die in dem TAINY xMOD gespeichert sind. *Download*: Lädt das Profil auf den Admin-PC. *Aktivieren*: Das TAINY xMOD übernimmt die Einstellungen des ausgewählten Konfigurationsprofils und arbeitet mit diesen weiter.

Löschen — Das Konfigurationsprofil wird gelöscht.

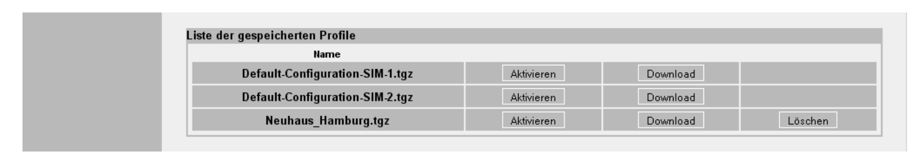
Das Profil *Default-Configuration.tgz* enthält eine Standard-Konfiguration und kann nicht gelöscht werden.

Standard-Konfigurationen

Geräte ohne Dual-SIM-Funktionalität enthalten eine Standard-Konfiguration (*Default-Configuration.tgz*), mit der die Konfiguration in den Auslieferzustand zurückversetzt werden kann. Das Zugangspasswort und im Gerät abgespeicherte Konfigurationen bleiben dabei erhalten. Es ist jedoch zu beachten, dass auch die lokale IP-Adresse zurückgesetzt wird und das Gerät somit nach Aktivieren einer Standard-Konfiguration ausschließlich über die IP-Adresse 192.168.1.1 erreichbar ist.

NUR Geräte der Produktvariante DS

Geräte der Produktvariante DS besitzen zwei Standard-Konfigurationen, je eine pro SIM-Karten-Steckplatz. Diese sind mit *Default-Configuration-SIM-1.tgz* und *Default-Configuration-SIM-2.tgz* bezeichnet. Sie besitzen dieselbe Funktion wie *Default-Configuration.tgz* in Geräten mit nur einer SIM-Karte und sind wie diese Standard-Konfiguration nicht löschbar:



Konfigurationsprofile per SSH laden und aktivieren.

Konfigurationsprofile können auch über den SSH-Zugang (siehe Kapitel 9.4) in das TAINY xMOD geladen und dort aktiviert werden.

Kopieren Sie dazu das Konfigurationsprofil (z.B. TAINY.tgz) per SSH in das Verzeichnis /webserver/profiles/.

Kopieren Sie danach eine Trigger-Datei mit folgenden Namen in das gleiche Verzeichnis:

<Konfigurationsprofil>@now.trigger

Sobald das TAINY xMOD diese Datei in dem Verzeichnis erkennt, wird das neue Konfigurationsprofil übernommen. Der Inhalt der Trigger-Datei spielt keine Rolle.

Beispiel:

Konfigurationsprofil: TAINY.tgz

Trigger-Datei: TAINY.tgz@now.trigger

3.9 Passwort ändern

Zugang > Authentifizierung > Lokal



Funktion

Der Zugang zum TAINY xMOD ist durch ein Zugangspasswort geschützt. Dieses Zugangspasswort schützt sowohl den Zugang über die

- lokale Schnittstelle auf die Web-Oberfläche und
- lokale Schnittstelle auf die SSH-Konsole

wie auch den Zugang über die verfügbare Funkverbindung (HSPA+, UMTS, EGPRS oder GPRS)

- per https auf die Web-Oberfläche und
- per ssh auf die SSH-Konsole

Zugangspasswort (Werkseinstellung)

Die Werkseinstellung für das TAINY xMOD lautet:

- Passwort: *root*
- Benutzername: *root (*kann nicht verändert werden)

Hinweis

Bitte ändern Sie das Passwort sofort nach Inbetriebnahme. Die werkseitige Voreinstellung ist allgemein bekannt und bietet keinen ausreichenden Schutz.

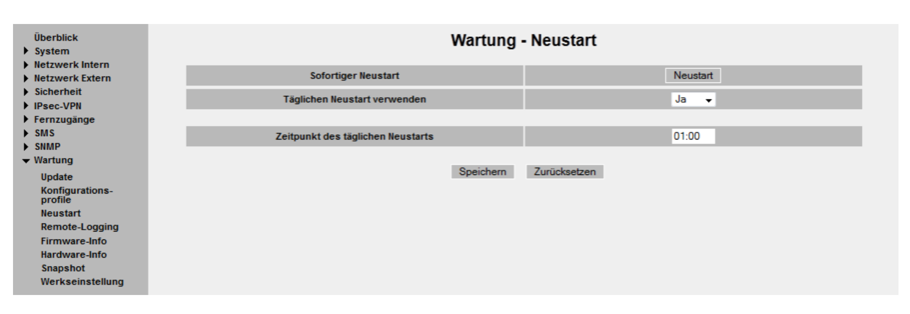
Neues Zugangspasswort (mit Wiederholung)

Um das Passwort zu ändern, geben Sie bei *Neues Zugangspasswort* das neu ausgewählte Passwort ein und wiederholen Sie die Eingabe im Feld *Neues Zugangspasswort (Wiederholung).*

Mit *Zurücksetzen* werden Ihre noch nicht gespeicherten Eingaben verworfen. Mit *Speichern* wird das neue Passwort übernommen.

3.10 Neustart

Wartung > Neustart



Funktion

Obwohl das TAINY xMOD für den Dauerbetrieb ausgelegt ist, kann es bei solch einem komplexen System zu Störungen kommen, oftmals ausgelöst durch äußere Einwirkung. Ein Neustart kann diese Störungen beheben.

Der Neustart setzt die Funktionen des TAINY xMOD zurück. Die aktuell im Gerät aktiven Einstellungen ändern sich nicht. Nach dem Neustart arbeitet das TAINY xMOD mit diesen Einstellungen weiter.

Sofortiger Neustart

Der Neustart wird sofort ausgeführt, wenn Sie auf *Neustart* klicken.

Täglichen Neustart verwenden

Der Neustart wird automatisch einmal am Tag ausgeführt, wenn Sie die Funktion mit *Ja* einschalten.

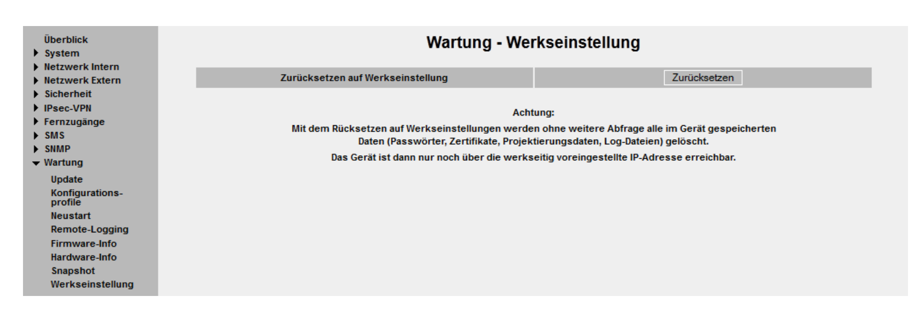
Geben Sie den *Zeitpunkt des täglichen Neustarts* an. Der Neustart erfolgt bei der angegebenen Systemzeit. Bestehende Verbindungen werden unterbrochen.

Werkseinstellung

Täglichen Neustart verwenden:	**Nein**
Zeitpunkt des täglichen Neustarts:	**01:00**

3.11 Werkseinstellung laden

Wartung > Werkseinstellung



Zurücksetzen auf Werkseinstellung

Das Betätigen der Schaltfläche *Zurücksetzen* lädt die werkseitigen Einstellungen, setzt die Passwörter zurück und löscht die gespeicherten Konfigurationsprofile und die archivierten Logbücher. TAINY xMOD-V3-Geräte löschen zusätzlich die gespeicherten Zertifikate.

Service-Taster

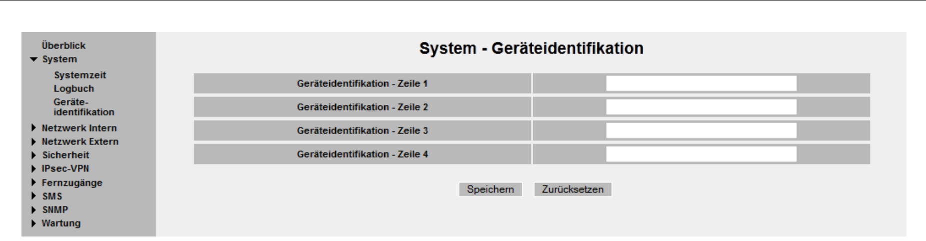
Das Zurücksetzen auf Werkseinstellungen kann auch über den Service-Taster ausgelöst werden (siehe Kapitel 2.5).

Standard-Konfiguration

Wenn nur die werkseitigen Einstellungen geladen werden sollen, ohne dass die Konfigurationsprofile und die archivierten Logbücher gelöscht werden, aktivieren Sie nur die Standard-Konfiguration wie in Kapitel 3.8 beschrieben. Bei TAINY xMOD-V3-Geräten werden bei diesem Vorgang auch die installierten Zertifikate gelöscht.

3.12 Geräteidentifikation

System > Geräteidentifikation



Geräteidentifikation – Zeile 1 - 4

Das TAINY xMOD bietet vier Textfelder, in denen beliebige Zeichenketten zum Beispiel zur Geräteidentifikation gespeichert werden können.

Die Textfelder können beschrieben und gelesen werden.

Die Textfelder sind jeweils auf 60 Zeichen begrenzt.

Zeichensatz

! $ % & ' ( ) * + , . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ _ ` a b c d e f g h i j k l m n o p q r s t u v w x y z { | }

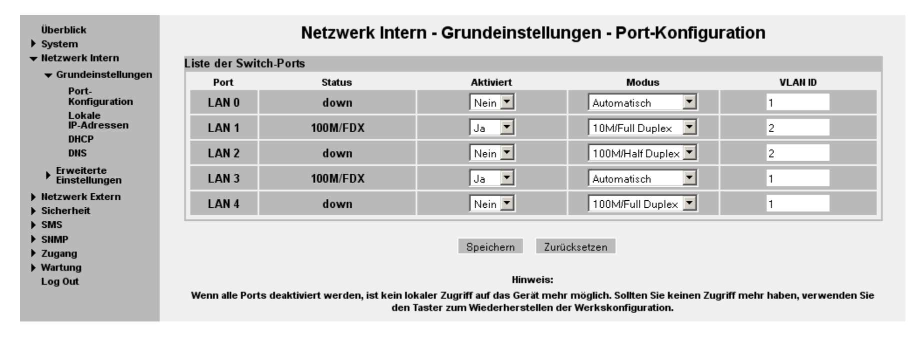
SNMP

Die vier Textfelder können mittels SNMP ausgelesen werden (siehe Kapitel 12.1).

4 Lokale Schnittstelle

4.1 Port-Konfiguration

Netzwerk Intern > Grundeinstellungen > Port-Konfiguration



Funktion

Jeder Ethernet-Port des TAINY xMOD kann hier getrennt aktiviert bzw. deaktiviert werden. Zusätzlich können die Eigenschaften der Ethernet-LAN-Schnittstelle festgelegt und die Schnittstellen in VLAN zusammengefasst werden.

Status

Zeigt die aktuelle Konfiguration von Datenrate und Übertragungsmodus der Schnittstelle an:

down	Schnittstelle nicht aktiv
10M/HDX	Schnittstelle konfiguriert für 10 Mbit / halbduplex
10M/FDX	Schnittstelle konfiguriert für 10 Mbit / vollduplex
100M/HDX	Schnittstelle konfiguriert für 100 Mbit / halbduplex
100M/FDX	Schnittstelle konfiguriert für 100 Mbit / vollduplex

Aktiviert

Wählen Sie *Ja* um die Schnittstelle zu aktivieren.

Modus

Dient zur Konfiguration von Datenrate und Übertragungsmodus der Schnittstelle:

Automatisch	Die Konfiguration der Schnittstelle wird automatisch mit der Gegenstelle ausgehandelt.
10M/HDX	Schnittstelle konfiguriert für 10 Mbit / halbduplex
10M/FDX	Schnittstelle konfiguriert für 10 Mbit / vollduplex
100M/HDX	Schnittstelle konfiguriert für 100 Mbit / halbduplex
100M/FDX	Schnittstelle konfiguriert für 100 Mbit / vollduplex

VLAN ID

Die VLAN-Funktion (Virtual Local Area Network) erlaubt es, die LAN-Schnittstellen des TAINY xMOD-x3 in verschiedene, unabhängige virtuelle Netzwerke aufzuteilen. Lokale Applikationen, die an LAN-Schnittstellen mit gleicher VLAN ID angeschlossen sind, können über das TAINY xMOD-x3 miteinander kommunizieren. Sind die VLAN IDs unterschiedlich, ist die Kommunikation untereinander nicht möglich.

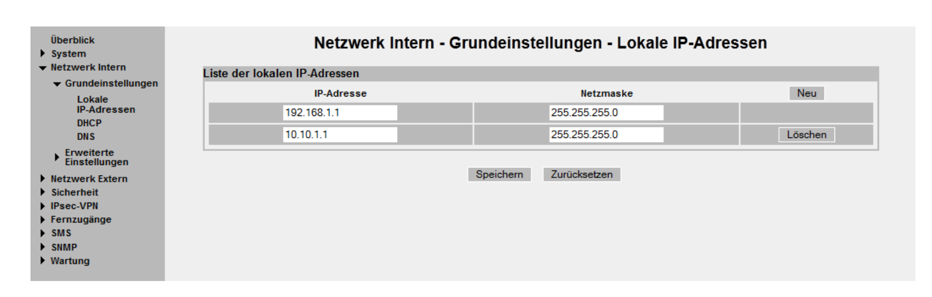
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Aktiviert	**Ja**
Modus	**Automatisch**
VLAN ID	**1**

4.2 IP-Adressen der lokalen Schnittstelle

Netzwerk Intern > Grundeinstellungen > Lokale IP-Adressen

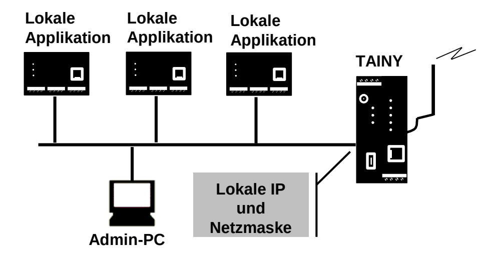


Lokale IP-Adresse laut Werkseinstellung: **192.168.1.1**

An dieser Stelle werden die IP-Adressen und die Netzmasken eingestellt unter denen das TAINY xMOD von lokalen Applikationen erreichbar ist. Werkseitig hat das TAINY xMOD folgende Einstellungen:

IP	192.168.1.1
Netzmaske	255.255.255.0

Diese werkseitig eingestellte IP-Adressen und Netzmaske kann frei verändert werden, sollten jedoch den geltenden Empfehlungen (RFC 1918) folgen.



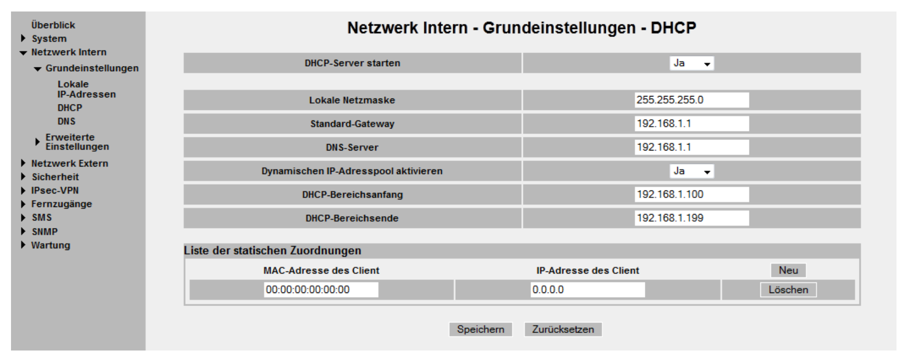
Sie können weitere Adressen festlegen, unter denen das TAINY xMOD von lokalen Applikationen erreicht werden kann. Dies ist dann hilfreich, wenn z.B. das lokale Netz in Subnetze unterteilt wird. Dann können mehrere lokale Applikationen aus verschiedenen Subnetzen das TAINY xMOD unter unterschiedlichen Adressen erreichen.

Neu Fügt weitere IP-Adressen und Netzmasken hinzu, die Sie wiederum ändern können.

Löschen Entfernt die jeweilige IP-Adresse und Netzmaske. Der erste Eintrag kann nicht gelöscht werden.

4.3 DHCP-Server zum lokalen Netz

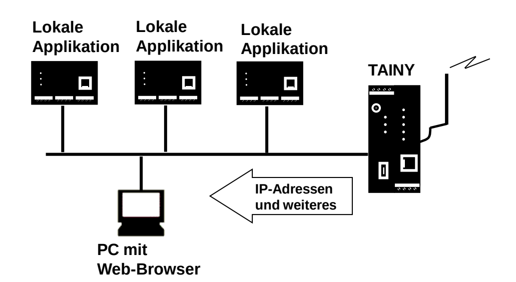
Netzwerk Intern > Grundeinstellungen > DHCP



DHCP Funktion

Das TAINY xMOD beinhaltet einen DHCP-Server (DHCP = Dynamic Host Configuration Protokoll). Ist die DHCP-Funktion des TAINY xMOD eingeschaltet und ist der DHCP-Server-Modus ausgewählt, weist der

DHCP-Server den Applikationen, die an der lokalen Schnittstelle des TAINY xMOD angeschlossen sind, automatisch die IP-Adressen, Netzmasken, das Gateway und den DNS-Server zu. Dazu muss bei den lokalen Applikationen das automatische Beziehen der IP-Adresse und der Konfigurationsparameter per DHCP aktiviert sein.



Alternativ kann das TAINY xMOD DHCP Anfragen von lokalen Applikationen auch über die WAN-Schnittstelle an entfernte DHCP-Server durchreichen von denen die Anfragen dann beantwortet werden. Dazu muss der DHCP-Relay-Modus ausgewählt werden (siehe Kapitel 4.4).

DHCP verwenden — Mit *DHCP verwenden – Ja* schalten Sie die DHCP-Funktionen des TAINY xMOD ein, mit *Nein* werden diese ausgeschaltet.

DHCP-Modus — Wählen Sie *DHCP-Server* um den internen DHCP-Server des TAINY xMOD einzuschalten. DHCP-Anfragen werden dann direkt vom TAINY xMOD beantwortet.

Wählen Sie *DHCP-Relay*, wenn das TAINY xMOD DHCP-Anfragen über die WAN-Schnittstelle an einen entfernten DHCP-Server weiterleiten soll (siehe Kapitel 4.4).

Lokale Netzmaske — Tragen Sie hier die lokale Netzmaske ein, die den lokalen Applikationen zugewiesen werden soll.

Standard-Gateway — Tragen Sie hier das Default-Gateway ein, das den lokalen Applikationen zugewiesen werden soll.

DNS-Server — Tragen Sie hier den DNS-Server ein, der den lokalen Applikationen zugewiesen werden soll.

Dynamischen IP-Adresspool aktivieren — Bei *Ja* werden die IP-Adressen, die der DHCP-Server des TAINY xMOD vergibt aus einem dynamischen Adresspool entnommen,

Bei *Nein* müssen die IP-Adressen unter *Statische Zuordnung* den MAC-Adressen der lokalen Applikationen zugeordnet werden.

DHCP-Bereichsanfang — Gibt die erste Adresse des dynamischen Adresspools an.

DHCP-Bereichsende — Gibt die letzte Adresse des dynamischen Adresspools an.

Statische Zuordnung

Bei Statischer Zuordnung der IP-Adressen, können Sie den MAC-Adressen lokaler Applikationen korrespondierende IP-Adressen fest zuweisen.

Liste der statischen Zuordnungen — Fordert eine lokale Applikation per DHCP die Zuweisung einer IP-Adresse, übermittelt die Applikation bei der DHCP-Anfrage seine MAC-Adresse. Ist dieser MAC-Adresse eine IP-Adresse statisch zugeordnet, weist TAINY xMOD der Applikation die korrespondierende IP-Adresse zu. Die Zuweisung findet über die *Liste der statischen Zuordnungen* statt.

MAC-Adresse des Clients –
MAC-Adresse der anfragenden lokalen Applikation

IP-Adresse des Clients –
zugeordnete IP-Adresse

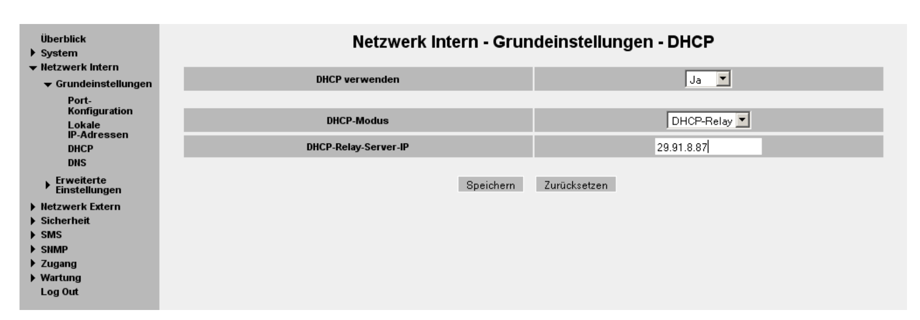
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

DHCP-Server starten	**Nein**
DHCP-Modus	**DHCP-Server**
Lokale Netzmaske	**255.255.255.0**
Standard-Gateway	**192.168.1.1**
DNS-Server	**192.168.1.1**
Dynamischen IP-Adresspool aktivieren	**Nein**
DHCP-Bereichsanfang	**192.168.1.100**
DHCP-Bereichsende	**192.168.1.199**
MAC-Adresse des Clients	**00:00:00:00:00:00**
IP-Adresse des Clients	**0.0.0.0**

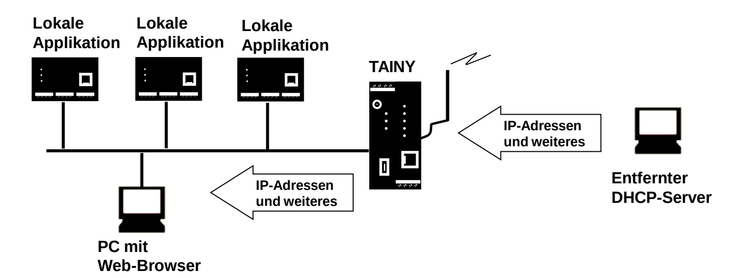
4.4 DHCP-Relay zum lokalen Netz

Netzwerk Intern > Grundeinstellungen > DHCP



DHCP Funktion

Das TAINY xMOD beinhaltet eine DHCP-Relay-Funktion (DHCP = Dynamic Host Configuration Protokoll). Ist die DHCP-Funktion des TAINY xMOD eingeschaltet und ist der DHCP-Relay-Modus ausgewählt, reicht das TAINY xMOD DHCP-Anfragen von lokalen Applikationen über die WAN-Schnittstelle an einen entfernten DHCP-Server durch, von dem die Anfragen dann beantwortet werden.



Alternativ verfügt das TAINY xMOD auch über einen internen DHCP-Server um DHCP-Anfragen zu beantworten (siehe Kapitel 4.3).

DHCP verwenden

Mit *DHCP verwenden – Ja* schalten Sie die DHCP-Funktionen des TAINY xMOD ein, mit *Nein* werden diese ausgeschaltet.

DHCP-Modus

Wählen Sie *DHCP-Relay*, wenn das TAINY xMOD DHCP-Anfragen über die WAN-Schnittstelle an einen entfernten DHCP-Server weiterleiten soll.

Wählen Sie *DHCP-Server* um den internen DHCP-Server des TAINY xMOD einzuschalten (siehe Kapitel 4.3).

DHCP-Relay-Server-IP

Geben Sie die IP-Adresse ein, unter der der entfernte DHCP-Server erreichbar ist.

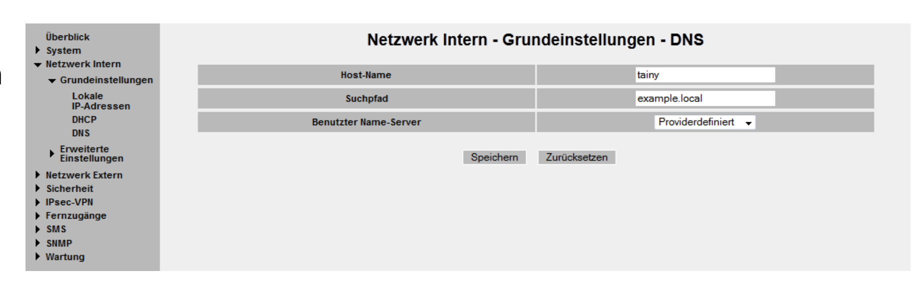
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

DHCP-Server starten	**Nein**
DHCP-Modus	**DHCP-Server**
DHCP-Relay-Server-IP	**0.0.0.0**

4.5 DNS zum lokalen Netz

Netzwerk Intern > Grundeinstellungen > DNS

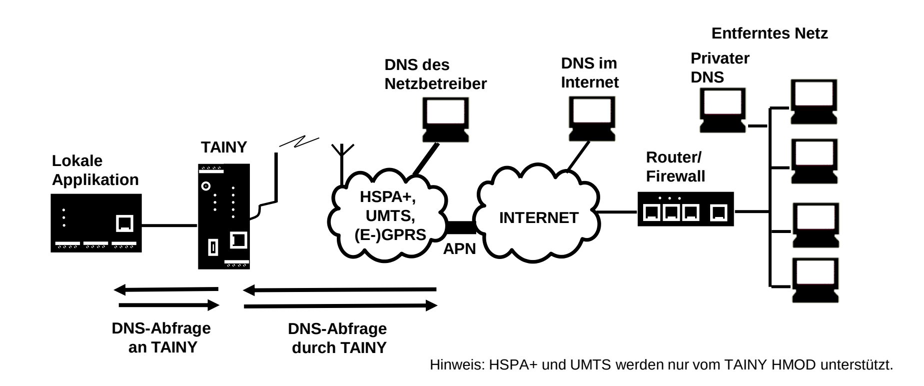


Funktion

Das TAINY xMOD stellt dem lokalen Netz einen Domain Name Server (DNS) bereit.

Tragen Sie in Ihrer lokalen Applikation die IP-Adresse des TAINY xMOD als Domain Name Server (DNS) ein, dann beantwortet das TAINY xMOD die DNS-Abfragen aus seinem Cache. Kennt es zu einer Domain-Adresse nicht die dazugehörige IP-Adresse, leitet das TAINY xMOD diese Abfragen weiter an einen externen Domain Name Server (DNS).

Die Zeitspanne, in der das TAINY xMOD eine Domain-Adresse im Cache behält, ist abhängig vom adressierten Host. Die DNS-Abfragen an einen externen Domain Name Server liefern außer der IP-Adresse auch die Lebensdauer dieser Information zurück.



Als externe Domain Name Server (DNS) können Server des Netzbetreibers, Server im Internet oder Server im privaten externen Netz verwendet werden.

Benutzter Name-Server

Wählen Sie aus, bei welchen Domain Name Server (DNS) das TAINY xMOD nachfragen soll:

Providerdefiniert	Beim Verbindungsaufbau zum Datenfunkdienst (HSPA+/UMTS/EGPRS/GPRS) übermittelt der Netzbetreiber automatisch eine oder mehrere DNS-Adressen.
Benutzerdefiniert	Sie wählen als Anwender Ihre(n) bevorzugten DNS aus. Die DNS können mit dem Internet verbunden sein oder es kann ein privater DNS in Ihrem Netz sein.

Liste der benutzerdefinierten Name-Server	Wenn Sie die Option *Benutzer definiert* gewählt haben, dann geben Sie bitte die IP-Adresse des ausgewählten DNS als *Server IP-Adresse* ein. Mit *Neu* können Sie weitere DNS hinzufügen, mit *Löschen* einen DNS entfernen.

Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Benutzter Name-Server	**Providerdefiniert**
Liste der benutzerdefinierten Name-Server	**-**
bei neuem Eintrag	**0.0.0.0**

4.6 Lokaler Host-Name

Netzwerk Intern > Grundeinstellungen > DNS

Das TAINY xMOD kann aus dem lokalen Netz, auch über einen Host-Namen adressiert werden. Legen Sie dazu einen Host-Namen fest, z.B. *myTAINY*.

Das TAINY xMOD kann dann zum Beispiel von einem Web-Browser als *myTAINY* aufgerufen werden.

Hinweis

Das Sicherheitskonzept des TAINY xMOD macht es erforderlich, dass für jede lokale Applikation, die diese Host-Namen-Funktion nutzen soll, eine ausgehende Firewall-Regel erstellt wird. Siehe Kapitel 6.1.

Wenn Sie kein DHCP, siehe Kapitel 4.3 verwenden, müssen im TAINY xMOD und in den lokalen Applikationen manuell identische Suchpfade eingetragen werden. Wenn Sie DHCP verwenden, erhalten die lokale Applikationen den im TAINY xMOD eingetragenen Suchpfad per DHCP.

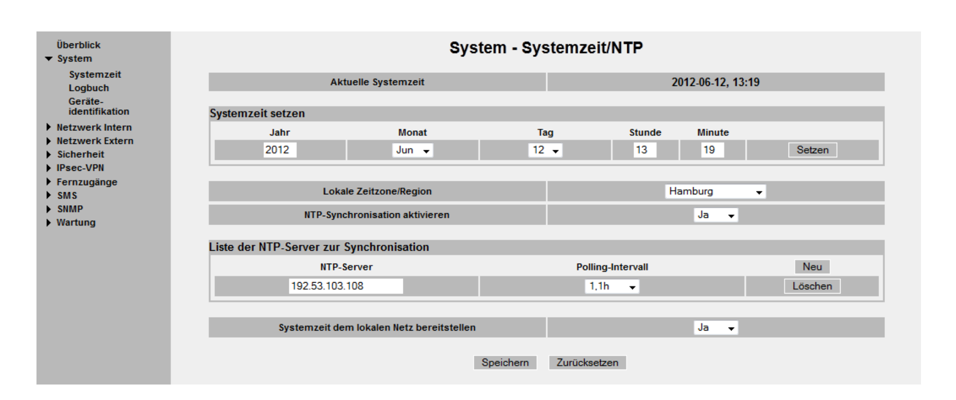
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Host-Name	**tainy**
Suchpfad	**example.local**

4.7 Systemzeit/NTP

System > Systemzeit/NTP



Systemzeit setzen

An dieser Stelle setzen Sie die Systemzeit für das TAINY xMOD. Diese Systemzeit wird:

- als Zeitstempel für alle Logbuch-Einträge benutzt und
- dient als Zeitbasis für alle zeitgesteuerten Funktionen.

Wählen Sie Jahr, Monat und Tag sowie Stunde und Minute.

NTP-Synchronisation aktivieren

Das TAINY xMOD kann die Systemzeit auch über NTP (= *Network Time Protokoll*) von einem Zeitserver beziehen. Im Internet gibt es eine Reihe von Zeitservern von denen die aktuelle Uhrzeit sehr präzise mittels NTP bezogen werden kann.

Lokale Zeitzone/ Region

Die NTP-Zeitserver übermitteln die UTC (= *Universal Time Coordinated*), d.h. die koordinierte Weltzeit. Wählen Sie eine Stadt in der Nähe des Standortes aus, an dem das TAINY xMOD arbeiten soll und legen Sie so die Zeitzone fest. Dann wird die Uhrzeit dieser Zeitzone als Systemzeit verwendet.

NTP-Server

Klicken Sie auf *Neu*, um einen NTP-Server hinzuzufügen und geben Sie die IP-Adresse eines solchen NTP-Servers ein oder verwenden Sie den ab Werk voreingestellten NTP-Server. Sie können parallel mehrere NTP-Server angeben.

Die Eingabe der NTP-Adresse als Host-Name (z.B. timeserver.org) ist nicht möglich.

Mit *Löschen* können Sie einen eingetragenen NTP-Server wieder entfernen.

Polling-Intervall

Die Zeitsynchronisation erfolgt zyklisch. Das Intervall, in dem die Synchronisation stattfindet, bestimmt das TAINY xMOD automatisch. Spätestens nach 36 Stunden findet erneut eine Synchronisation statt. Das Polling-Intervall legt fest, wie lange das TAINY xMOD mindestens bis zur nächsten Synchronisation wartet.

Hinweis

Die Synchronisation der Systemzeit über NTP verursacht ein zusätzliches Datenaufkommen auf der Datenfunk-Verbindung. Abhängig von den gewählten Einstellungen kann das zusätzliche Datenaufkommen 120 kByte im Monat und mehr betragen. Je nach Teilnehmervertrag mit dem GSM-Netzbetreiber sind damit erhöhte Kosten verbunden.

Systemzeit dem lokalen Netz bereitstellen

Das TAINY xMOD kann selber als NTP-Zeitserver für die Applikationen dienen, die an seiner lokalen Netzwerkschnittstelle angeschlossen sind. Zur Aktivierung dieser Funktion wählen Sie *Ja*.

Der NTP-Zeitserver im TAINY xMOD ist über die eingestellte lokale IP-Adresse des TAINY xMOD erreichbar, siehe Kapitel 4.1.

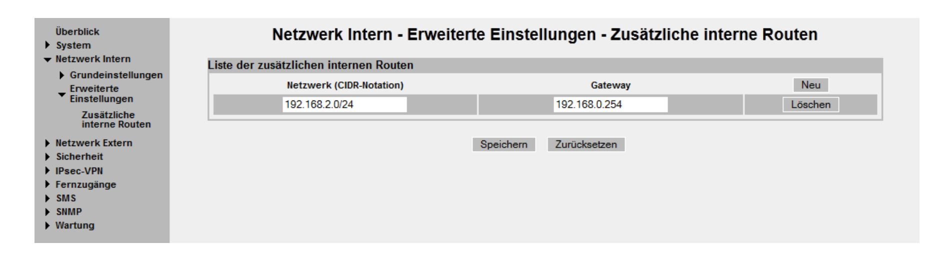
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Lokale Zeitzone	**UTC**
NTP Synchronisation aktivieren	**Nein**
NTP-Server	**192.53.103.108**
Polling-Intervall	**1.1 Stunden**
Systemzeit dem lokalen Netz bereitstellen	**Nein**

4.8 Zusätzliche interne Routen

Netzwerk Intern > Erweiterte Einstellungen > Zusätzliche interne Routen



Funktion

Teilt sich das lokale Netz in Subnetze auf, können Sie zusätzliche Routen definieren.

Siehe auch Kapitel 16.

Um eine weitere Route zu einem Subnetz festzulegen, klicken Sie *Neu*.
Geben Sie folgendes an:
- die IP-Adresse des Subnetzes (Netzwerkes), ferner
- die IP-Adresse des Gateways, über das das Subnetz angeschlossen ist.
Sie können beliebig viele interne Routen festlegen.

Möchten Sie eine interne Route löschen, klicken Sie *Löschen*.

Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

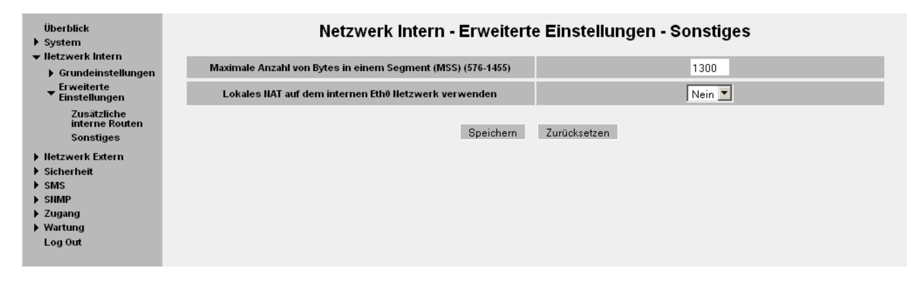
Zusätzliche interne Routen **-**

Vorgabe für neue Routen:

Netzwerk (CIDR-Notation)	**192.168.2.0/24**
Gateway	**192.168.0.254**

4.9 Erweiterte Einstellungen für das interne Netzwerk

Netzwerk Intern > Erweiterte Einstellungen > Sonstiges



Funktion

Dieses Untermenü enthält erweiterte Einstellungen zur Datenverarbeitung im lokalen Netzwerk

Maximale Anzahl von Bytes in einem Segment (MSS)

Mit der Maximum Segment Size (MSS) wird die maximale Anzahl von Nutzdaten-Bytes festgelegt, die ein TCP-Segment enthalten darf.

Der gültige Wertebereich für diesen Parameter liegt bei 576 bis 1455.

Lokales NAT auf dem internem Netzwerk verwenden	Beim lokalen NAT (Network Address Translation) auf der internen Schnittstelle werden alle Datenpakete, die im TAINY xMOD von der externen WAN-Schnittstelle an das interne Netzwerk weitergeleitet werden, mit der lokalen IP-Adresse des TAINY xMOD als Quelladresse versehen. Dies kann für bestimmte Applikationen notwendig sein. Wählen Sie *Ja*, wenn Sie lokales NAT auf dem internen Netztwerk aktivieren wollen. Wählen Sie *Nein*, um das lokale NAT auf dem internen Netzwerk zu deaktivieren.

Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Maximale Anzahl von Bytes pro Segment	**1300**
Lokales NAT auf dem internen Netzwerk verwenden	**Nein**

5 Externe Schnittstelle

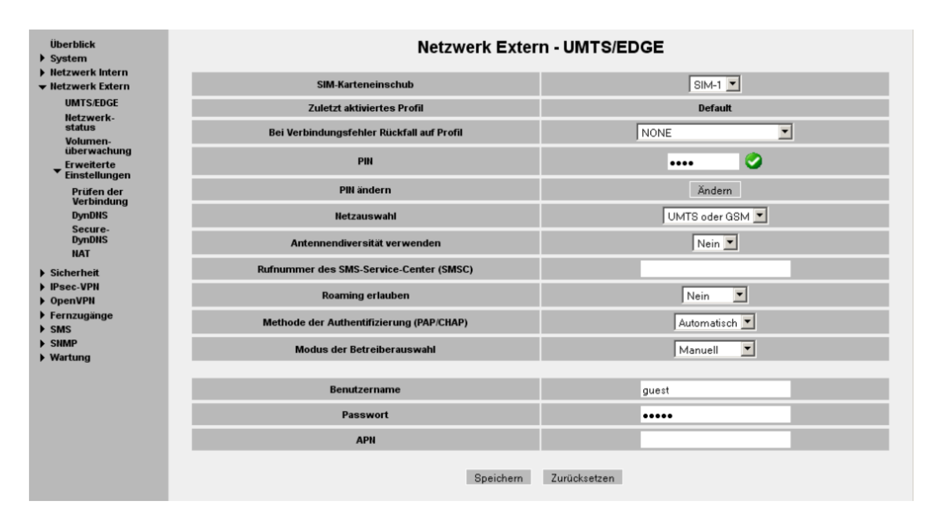
5.1 Netzauswahl und Zugangsparameter für UMTS bzw. EGPRS und GPRS

Netzwerk Extern > UMTS/EDGE

NUR TAINY HMOD

Netzwerk Extern > EDGE/GPRS

NUR TAINY EMOD

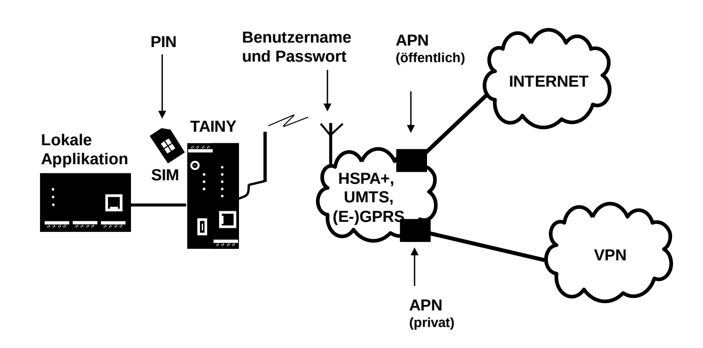


Funktion

Das TAINY HMOD verwendet als Datenfunkdienst HSPA+, UMTS data, EGPRS oder GPRS zur Kommunikation mit dem externen Netz. Auszuwählen ist der Typ des Mobilfunknetzes (UMTS oder GSM).

Das TAINY EMOD verwendet als Datenfunkdienst EGPRS oder GPRS. Für den Zugang zu diesen IP-Mobillfunkdiensten und zum grundlegenden Funknetz sind Zugangsparameter erforderlich, die Sie von Ihrem Mobilfunkbetreiber erhalten.

Die PIN schützt die SIM-Karte vor unbefugter Benutzung. Benutzername und Passwort schützen den Zugang zum Datenfunkdienst und der APN (Access Point Name) definiert den Übergang vom Datenfunkdienst zu weiteren verbundenen IP-Netzen, z.B. einen öffentlichen APN zum Internet oder einen privaten APN zu einem Virtual Private Network (VPN).



SIM-Karteneinschub

NUR PODUKTVARIANTE DS (Dual SIM)

Bei der Konfiguration eines TAINY der Gerätevariante DS (Dual SIM) legen Sie hier fest, für welche der beiden SIM-Karten im Gerät die Konfiguration gültig ist.

Für weitere Informationen zur Gerätevariante DS siehe Kapitel 14

Zuletzt aktiviertes Profil

Zeigt den Namen des zuletzt im TAINY xMOD aktivierten Konfigurations-profils an.

Wurde seit Inbetriebnahme noch kein Konfigurationsprofil aktiviert oder das Gerät wieder in den Werkszustand zurückversetzt (siehe 3.11) wird hier *Default* angegeben.

Bei Verbindungsfehler Rückfall auf Profil

Legen Sie hier das Profil fest, zu dem das Gerät wechseln soll, sollte es keine Verbindung zum Datenfunkdienst (HSPA+, UMTS, EGPRS oder GPRS) herstellen können. Mit diesem Profil wird dann ein neuer

Verbindungsversuch zum Datenfunkdienst durchgeführt.

Enthält der Parameter den Wert ***NONE***, ist der Rückfall deaktiviert (siehe Kapitel 15)

PIN

Geben Sie hier die PIN Ihrer SIM-Karte ein. Sie erhalten die PIN von Ihrem Netzbetreiber.

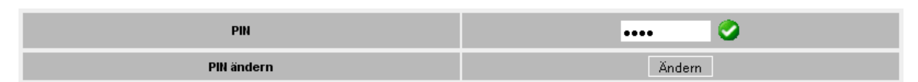
Das TAINY xMOD arbeitet auch mit PIN-losen SIM-Karten, hierfür geben Sie bitte ***NONE*** ein. Das Eingabefeld zeigt in diesem Fall keinen Wert an.

Hinweis

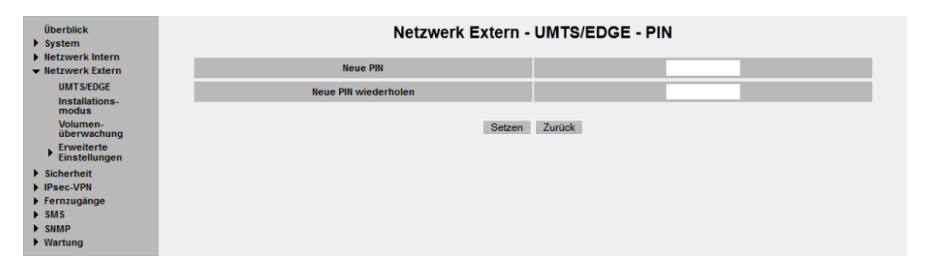
Ist hier keine PIN eingetragen, wird das Eingabefeld nach dem Speichern rot umrandet.

PIN ändern

Um die PIN auf der SIM-Karte zu ändern, betätigen Sie die Schaltfläche *Ändern*.



Es öffnet sich ein Untermenü.



Neue PIN

Geben Sie hier die neue PIN ein.

Neue PIN wiederholen

Geben Sie hier die neue PIN zur Bestätigung nochmals ein.

Hinweis

Ist die PIN-Abfrage bei der eingelegten SIM-Karte deaktiviert (PIN-lose Karte), kann die PIN nicht aktiviert bzw. geändert werden.

Netzauswahl

NUR TAINY HMOD

Das TAINY HMOD kann sich wahlweise mit UMTS- oder GSM-Mobilfunknetzen verbinden.

- UMTS (mit den Diensten UMTS data und HSPA+)
- GSM (mit den Diensten EGPRS, GPRS und CSD)

Bei der Einstellung *UMTS oder GSM* wählt das TAINY HMOD nach Verfügbarkeit vorrangig ein UMTS-Netz aus. Falls nicht erreichbar wird ein GSM-Netz verwendet.

Bei der Einstellung *Nur UMTS* wählt das TAINY HMOD in jedem Fall ein UMTS-Netz aus.

Bei der Einstellung *Nur GSM* wählt das TAINY HMOD in jedem Fall ein GSM-Netz aus.

Antennendiversität verwenden

NUR TAINY HMOD

Antennendiversität verwenden	Nein

Zur Verbesserung der Mobilfunk-**Empfangsqualität** kann eine zusätzliche Antenne zugeschaltet werden (Antennendiversität)

Nein	Wählen Sie *Nein*, um die Antennendiversität zu deaktivieren
Ja	Wählen Sie *Ja*, um die Antennendiversität zu aktivieren

Rufnummer des SMS-Service-Center (SMSC)

TAINY xMOD nutzt auch den Short Message Service (SMS) von GSM. Sie können ein spezielles SMS-Center festlegen.

Damit die SMS-Funktion sicher funktioniert, tragen Sie hier die Rufnummer des Service-Center ein. Ohne Eintrag an dieser Stelle wird das Standard-SMS-Service-Center Ihres Netzbetreibers verwendet. Durch das Fehlen des Eintrags kann es zu Fehlfunktionen kommen.

Achtung:

Wird keine Rufnummer für das SMS-Center eingetragen, oder erfolgt der Eintrag nicht in internationalem Format (z.B. +49…) kann der SMS-Versand scheitern.

Roaming erlauben

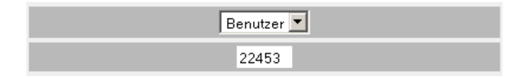
Roaming erlauben	Nein

Das TAINY xMOD unterstützt folgende Roaming-Modi:

Nein — Wählen Sie *Nein*, wenn sich das TAINY xMOD ausschliesslich in das Heimatnetz, d.h. in das Mobilfunknetz einbuchen soll, dessen SIM-Karte eingelegt ist.

Ja — Wählen Sie *Ja*, wenn sich das TAINY xMOD auch in die Partnernetze des Heimatnetzes einbuchen darf, sollte das Heimatnetz nicht oder schlechter erreichbar sein.

Benutzer — Im Modus *Benutzer* wird vom Anwender über den Parameter *Festlegen der Location Area Identity (MCC/MNC)* eine Netz-ID definiert, in deren Netzwerk sich das TAINY xMOD ausschließlich einbuchen darf. Andere verfügbare Mobilfunknetze, auch das Heimatnetz der SIM-Karte, werden vom TAINY xMOD in diesem Modus ignoriert.



Warnung

Bucht sich das TAINY xMOD in ein Partnernetz ein (Roaming) kann dies zu erheblichen Mehrkosten führen.

Methode der Authentifizierung PAP/CHAP

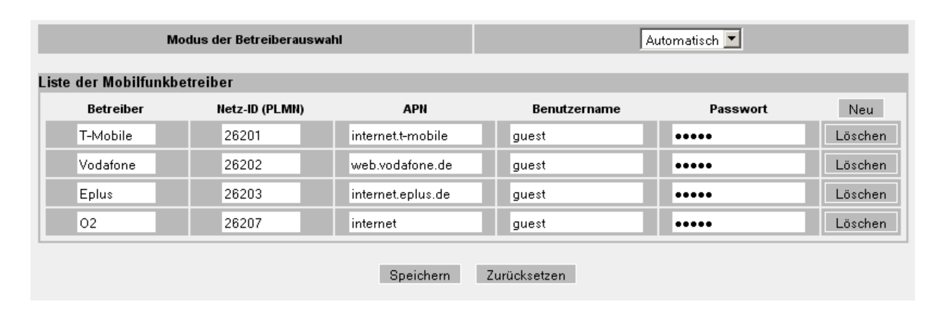
Für die Anmeldung am Datenfunkdienst (HSPA+, UMTS, EGPRS oder GPRS) werden zwei verschiedene Verfahren (PAP und CHAP) genutzt. In der Regel erfolgt die Auswahl des Verfahrens automatisch. Soll ein bestimmtes Verfahren benutzt werden, so kann die Auswahl manuell erfolgen. Wählen Sie aus zwischen Auto, PAP oder CHAP.

Modus der Betreiberauswahl - Manuell



Ist als Modus der Betreiberauswahl *Manuell* ausgewählt, geben Sie *Benutzername*, *Passwort* und *APN* für die UMTS- bzw. GSM-Dienste händisch ein.

Modus der Betreiberauswahl - Automatisch



Ist als Modus der Betreiberauswahl *Automatisch* ausgewählt, werden die Zugangsdaten für den UMTS- oder GSM-Dienste automatisch anhand der Net-ID der SIM-Karte aus der *Liste der Mobilfunkbetreiber* ausgewählt. Es können mehrere Einträge in der Liste angelegt werden. Die Anzahl ist nicht beschränkt, mehr als 10 Einträge sollten aber vermieden werden.

Mit *Neu* kann ein neuer Eintrag hinzugefügt werden. Mit *Löschen* werden Einträge entfernt.

Betreiber (nur bei automatischer Betreiberauswahl)

Geben Sie hier als Freitext eine Bezeichnung für den UMTS- oder GPRS-Dienst an, beispielsweise den Namen des Mobilfunkbetreibers (z.B. Vodafone, Eplus, mein GPRS-Zugang).

Net-ID (PLMN) (nur bei automatischer Betreiberauswahl)

Geben Sie hier die Identifikations-Nummer des Mobilfunkbetreibers ein, auf die sich die UMTS- oder GPRS-Zugangsdaten in der gleichen Zeile der Liste der Provider beziehen.

Jeder GSM/GPRS-Netzbetreiber hat eine weltweit einmalig vergebene Identifikations-Nummer. Diese ist auf der SIM-Karte gespeichert. Das TAINY xMOD liest diese Net-ID von der SIM-Karte und wählt die entsprechenden UMTS- oder GPRS-Zugangsdaten aus der Liste der Mobilfunkbetreiber.

Sie finden die NET-ID auf unserer Web-Seite www.neuhaus.de, in den Unterlagen Ihres GSM/GPRS-Netzbetreibers, auf seiner Internetseite oder erfragen ihn bei dessen Hotline (Stichwort MCC/MNC).

APN

Geben Sie hier den Namen des Übergangs vom Datenfunkdienst (HSPA+, UMTS, EGPRS oder GPRS) zu weiteren Netzen ein (TAINY HMOD max. 100 Zeichen; TAINY EMOD max 30 Zeichen).

Sie finden den APN in den Unterlagen Ihres Mobilfunkbetreibers, auf seiner Internetseite oder erfragen ihn bei dessen Hotline.

Benutzername

Geben Sie hier den Benutzername für den Datenfunkdienst (HSPA+, UMTS, EGPRS oder GPRS) ein (max. 127 Zeichen). Einige Mobilfunkbetreiber verzichten auf die Zugangskontrolle durch Benutzername und/oder Passwort. In diesem Fall tragen Sie in das jeweilige Feld *gast* ein.

Passwort

Geben Sie hier das Passwort für den Datenfunkdienst (HSPA+, UMTS, EGPRS oder GPRS) ein (max. 127 Zeichen). Einige Mobilfunkbetreiber verzichten auf die Zugangskontrolle durch Benutzername und/oder Passwort. In diesem Fall tragen Sie in das jeweilige Feld *gast* ein.

Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

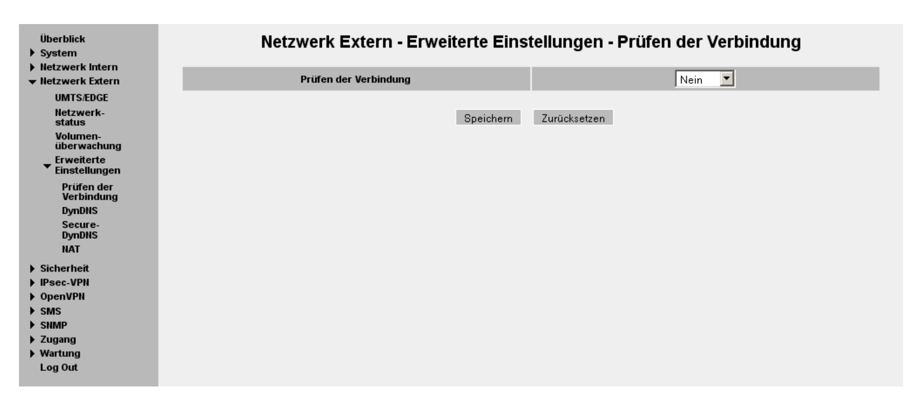
NUR PODUKTVARIANTE DS (Dual SIM)

SIM-Karteneinschub	**SIM 1**
Zuletzt aktiviertes Profil	**Default**
Bei Verbindungsfehler Rückfall auf	**NONE**

	Profil	
	PIN	**(leer)**
Nur TAINY HMOD	Netzauswahl	**UMTS oder GSM**
Nur TAINY HMOD	Antennendiversität verwenden	**Nein**
	Rufnummer des SMS-Service-Center (SMSC)	**(leer)**
	Roaming erlauben	**Nein**
	Methode der Authentifizierung PAP/CHAP	**Automatisch**
	Modus der Betreiberauswahl	**Automatisch**
Modus der Betreiberauswahl - Manuell	Benutzername	**guest**
	Passwort	**guest**
	APN	**(leer)**
Modus der Betreiberauswahl - Automatisch	1. Provider	**T-Mobile**
	Net-ID	**26201**
	APN	**internet.t-mobile**
	Benutzername	**guest**
	Passwort	**guest**
	2. Provider	**Vodafone**
	Net-ID	**26202**
	APN	**web.vodafone.de**
	Benutzername	**guest**
	Passwort	**guest**
	3. Provider	**Eplus**
	Net-ID	**26203**
	APN	**internet.eplus.de**
	Benutzername	**guest**
	Passwort	**guest**
	4. Provider	**O2**
	Net-ID	**26207**
	APN	**internet**
	Benutzername	**guest**
	Passwort	**guest**
	n. Provider	**NONE**
	Net-ID	**NONE**
	APN	**NONE**
	Benutzername	**guest**

Passwort	**guest**

5.2 Überwachung der Datenfunkdienst-Verbindung



Funktion

Mit der Funktion *Prüfen der Verbindung* überprüft das TAINY xMOD seine Verbindung zum Datenfunkdienst (HSPA+, UMTS, EGPRS oder GPRS) und zu den angeschlossenen externen Netzen, wie z.B. dem Internet oder einem Intranet. Dazu sendet das TAINY xMOD in regelmäßigen Zeitabständen Ping-Pakete (ICMP) an einen oder mehrere Hosts im zu überwachenden Netzwerk.

Das TAINY xMOD unterstützt folgende Modi:

Liste — Das TAINY xMOD sendet Ping-Pakete an bis zu vier Gegenstellen (Ziel-Hosts). Erhält das TAINY xMOD von mindestens einer der adressierten Gegenstellen eine Antwort, ist das TAINY xMOD noch mit dem Datenfunkdienst (HSPA+, UMTS, EGPRS oder GPRS) verbunden und betriebsbereit (siehe Kapitel 5.2.1).

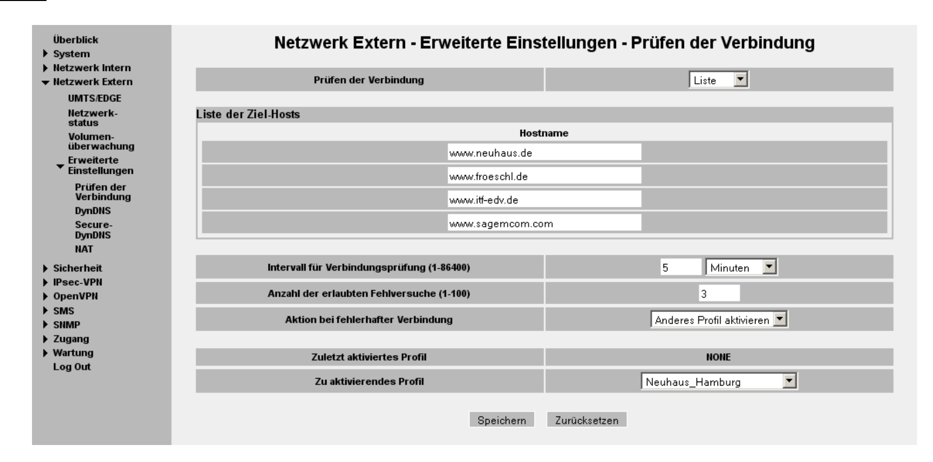
Statistik — Das TAINY xMOD sendet zyklisch eine einstellbares Anzahl von Ping-Paketen (*Burst*) an genau einen Ziel-Host und beobachtet das Antwortverhalten über einen festgelegten Zeitraum. Wird über diesen Beobachtungszeitraum eine festgelegte Quote an Antworten (*Erfolgsschwelle*) zurückerhalten, gilt die Prüfung als bestanden und das Gerät als mit dem Datenfunkdienst verbunden (siehe Kapitel 5.2.2).

Das Senden der Ping-Pakete geschieht unabhängig von den Nutzdaten-Verbindungen.

Einige Netzbetreiber unterbrechen Verbindungen bei Inaktivität. Dem wird durch die Funktion *Prüfen der Verbindung* ebenfalls vorgebeugt.

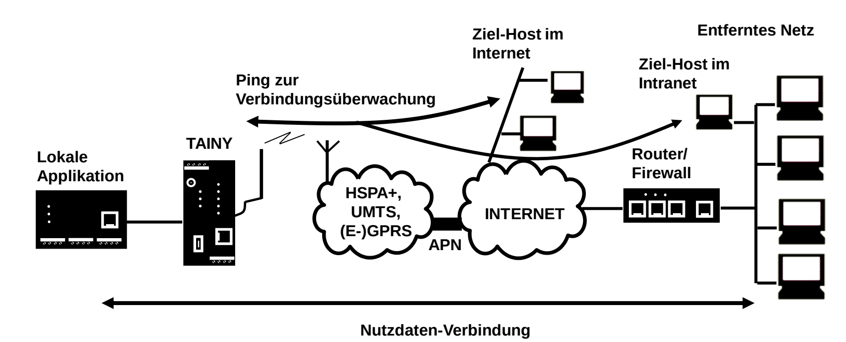
5.2.1 Modus „Liste“

Netzwerk Extern > Erweiterte Einstellungen > Prüfen der Verbindung



Funktion

Im Modus *Liste* sendet das TAINY xMOD in regelmäßigen Zeitabständen Ping-Pakete (ICMP) an bis zu vier Gegenstellen (Ziel-Hosts). Dies geschieht unabhängig von den Nutzdaten-Verbindungen. Erhält das TAINY xMOD auf einen solchen Ping von mindestens einer der adressierten Gegenstellen eine Antwort, ist das TAINY xMOD noch mit dem Datenfunkdienst (HSPA+, UMTS, EGPRS oder GPRS) verbunden und betriebsbereit.



Hinweis: HSPA+ und UMTS werden nur vom TAINY HMOD unterstützt.

Warnung

Durch das Versenden der Ping-Pakete (ICMP) steigt die Anzahl der über den Datenfunkdienst (HSPA+, UMTS, EGPPS oder GPRS) gesendeten und empfangenen Daten. Abhängig von den gewählten Einstellungen kann das zusätzliche Datenaufkommen 2,5 MByte im Monat (Ping an IP-Adresse) bzw. 6 Mbyte im Monat (Ping an Host-Namen) und mehr betragen. Dies kann zu erhöhten Kosten führen.

Prüfen der Verbindung

Mit *Liste* wird der Modus *Liste* eingeschaltet.

Liste der Ziel-Hosts - Host-Name

Wählen Sie bis zu vier Gegenstellen aus, denen das TAINY xMOD im Rahmen der Verbindungsprüfung Ping-Kommandos schicken soll. Die Gegenstellen müssen ständig erreichbar sein und Ping-Pakete beantworten.

Hinweis

Vergewissern Sie sich, dass sich die ausgewählten Gegenstellen nicht „belästigt“ fühlen.

Intervall für Verbindungsprüfung

Legt das Intervall fest, mit dem die Ping-Pakete der Verbindungsüber-wachung vom TAINY xMOD versendet werden. Der eingegebene Wert wird über das Auswahlmenü als Minuten- oder Sekundenwert festgelegt.

Anzahl der erlaubten Fehlversuche	Legt fest, wie oft es vorkommen darf, dass alle Ping-Pakete eines Intervalls nicht beantwortet werden, d.h. dass keine der angepingten Gegenstellen antwortet, bevor die festgelegte Aktion durchgeführt wird.	
Aktion bei fehlerhafter Verbindung	*Verbindung erneuern*	Das TAINY xMOD stellt erneut die Verbindung zum Datenfunkdienst (HSPA+, UMTS, EGPRS oder GPRS) her, falls die gesendeten Ping-Pakete nicht beantwortet wurden.
	Neustart des Gerätes	Das TAINY xMOD führt einen Neustart durch, falls die gesendeten Ping-Pakete nicht beantwortet wurden.
	Anderes Profil aktivieren	Das TAINY xMOD lädt ein anderes Profil, falls die gesendeten Ping-Pakete nicht beantwortet wurden, und versucht sich über dieses ins Netz eines Datenfunkdienstes einzuwählen. Das zu aktivierende Profil kann festgelegt werden, sobald die Aktion *Anderes Profil aktivieren* ausgewählt wurde.

Zuletzt aktiviertes Profil	default
Zu aktivierendes Profil	NONE

Zuletzt aktiviertes Profil	Zeigt den Namen des zuletzt im TAINY xMOD aktivierten Konfigurationsprofils an.
Zu aktivierendes Profil	Legen Sie hier das Profil fest, zu dem gewechselt wird, sollte die Verbindungsprüfung fehlschlagen (Es können nur Profile gewählt werden, die bereits im Gerät abgespeichert sind).

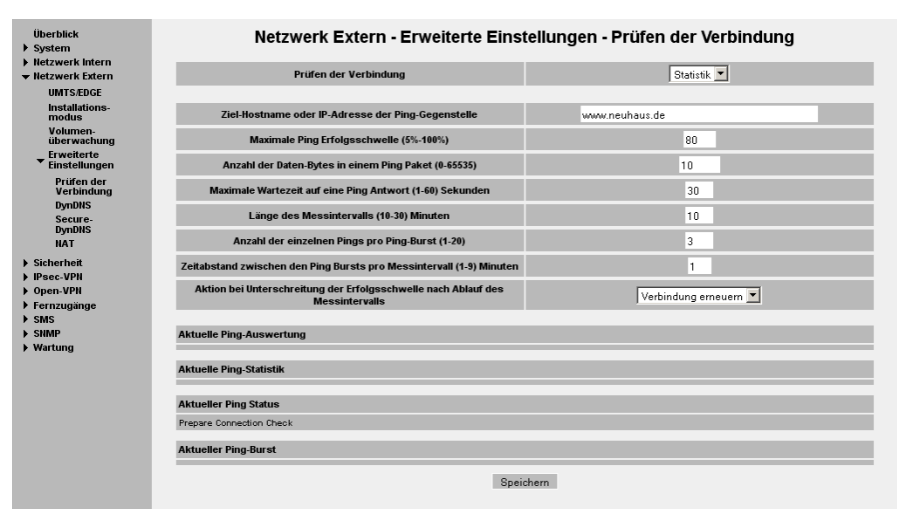
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Prüfen der Verbindung	**Nein (Ausgeschaltet)**
Host-Name	**-**
Intervall für Verbindungsprüfung	**5 (Minuten)**
Anzahl der erlaubten Fehlversuche	**3 (Fehlversuche)**
Aktion bei fehlerhafter Verbindung	**Verbindung erneuern**
Zu aktivierendes Profil	**NONE**

5.2.2 Modus „Statistik“

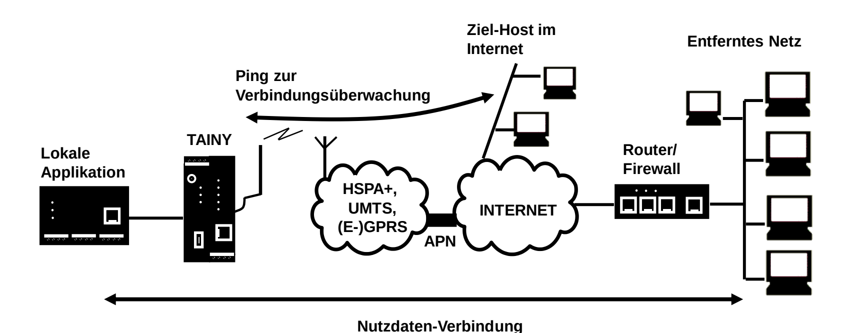
Netzwerk Extern > Erweiterte Einstellungen > Prüfen der Verbindung



Funktion

Im Modus *Statistik* sendet das TAINY xMOD in regelmäßigen Zeitab-

ständen Ping-*Bursts* an genau eine Gegenstelle (Ziel-Host). Mit „Burst“ wird das Versenden eines Ping-Pakets oder mehrerer Ping-Pakete direkt hintereinander bezeichnet.



Hinweis: HSPA+ und UMTS werden nur vom TAINY HMOD unterstützt.

Das Antwortverhalten der Gegenstelle wird - anders als beim *Liste*-Modus - über einen einstellbaren Zeitraum, das *Messintervall*, beobachtet.

Dabei setzt das TAINY xMOD nach Ablauf des Messintervalls die Anzahl aller innerhalb des Messintervalls erhaltenen Ping-Antworten ins Verhältnis zur Anzahl aller abgesendeten Ping-Pakete.

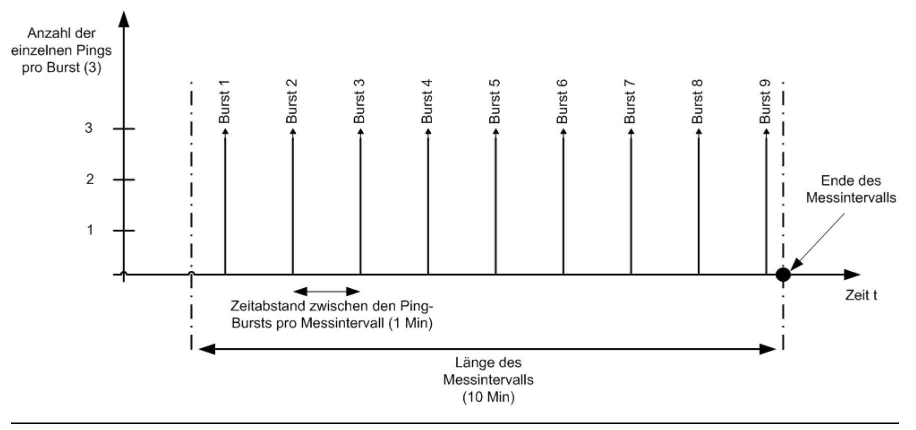
Das Ergebnis dieser Berechnung wird mit der einstellbaren *Erfolgsschwelle* verglichen. Ist diese Schwelle erreicht oder überschritten, gilt das TAINY xMOD als noch mit dem Datenfunkdienst (HSPA+, UMTS, EGPRS oder GPRS) verbunden und betriebsbereit.

Die statistische Auswertung, die durch Einträge ins Logbuch ergänzt wird, gibt darüber hinaus Auskunft über die Qualität einer bestehenden Verbindung.

Die Verbindungsprüfung wird unabhängig von bestehenden Nutzdaten-Verbindungen durchgeführt.

Zeitverhalten

Die folgende Grafik bietet einen Überblick über das Zeitverhalten des TAINY xMOD im Modus *Statistik*. In diesem Beispiel beträgt das Messintervall 10min, es werden im einminütigen Abstand aus jeweils drei Ping-Kommandos bestehende Bursts abgesetzt:



Warnung

Durch das Versenden der Ping-Pakete (ICMP) steigt die Anzahl der über den Datenfunkdienst (HSPA+, UMTS, EGPPS oder GPRS) gesendeten und empfangenen Daten. Abhängig von den gewählten Einstellungen (Zeitverhalten, Anzahl der Ping-Kommandos pro Burst, Länge der Ping-Pakete, ...) kann das zusätzliche Datenaufkommen mehrere MByte im Monat betragen.

Dies kann zu erhöhten Kosten führen.

Parametrierung

Netzwerk Extern - Erweiterte Einstellungen - Prüfen der Verbindung

Prüfen der Verbindung	Statistik
Ziel-Hostname oder IP-Adresse der Ping-Gegenstelle	www.neuhaus.de
Maximale Ping Erfolgsschwelle (5%-100%)	80
Anzahl der Daten-Bytes in einem Ping Paket (0-65535)	10
Maximale Wartezeit auf eine Ping Antwort (1-60) Sekunden	30
Länge des Messintervalls (10-30) Minuten	10
Anzahl der einzelnen Pings pro Ping-Burst (1-20)	3
Zeitabstand zwischen den Ping Bursts pro Messintervall (1-9) Minuten	1
Aktion bei Unterschreitung der Erfolgsschwelle nach Ablauf des Messintervalls	Verbindung erneuern

Prüfen der Verbindung

Mit *Statistik* wird der Modus *Statistik* eingeschaltet.

Ziel-Hostname oder IP-Adresse der Ping-Gegenstelle

Geben Sie den Hostnamen oder die IP-Adresse der Gegenstelle an, der das TAINY xMOD im Rahmen der Verbindungsprüfung Ping-Kommandos schicken soll. Die Gegenstelle muss ständig erreichbar sein und Ping-Pakete beantworten.

Hinweis

Vergewissern Sie sich, dass sich die ausgewählte Gegenstelle durch die Ping-Pakete nicht „belästigt“ fühlt.

Ping-Erfolgsschwelle

Legen Sie hier die Schwelle für erfolgreiche Ping-Tests fest, die am Ende des Messintervalls erreicht oder überschritten sein muss, damit das TAINY xMOD als mit dem WAN verbunden und betriebsbereit deklariert wird.

Der Wertebereich des Parameters ist 5% bis 100%.

Anzahl der Daten-Bytes in einem Ping-Paket

Legen Sie hier in Byte die Länge der Ping-Pakete fest, die zum Prüfen der Verbindung verschickt werden sollen.

Der Wertebereich des Parameters ist 0 bis 65535.

Maximale Wartezeit auf eine Ping-Antwort

Legen Sie hier die Zeit in Sekunden fest, innerhalb der eine Antwort auf ein verschicktes Ping-Paket beim TAINY xMOD eintreffen muss, damit dieses Ping-Paket als erfolgreich beantwortet gewertet wird.

Der Wertebereich des Parameters ist 1s bis 60s.

Länge des Messintervalls

Legt die Länge des Messintervalls in Minuten fest

Der Wertebereich des Parameters ist 10min bis 30min.

Anzahl der einzelnen Pings pro Ping-Burst

Im Modus *Statistik* werden in einem einstellbaren Intervall Ping-Bursts abgesetzt. Legen Sie hier fest, wie viele Ping-Pakete pro Burst abgesetzt werden sollen.

Der Wertebereich des Parameters ist 1 bis 20.

Zeitabstand zwischen den Ping-Bursts pro Messintervall

Legen Sie hier fest, in welchem zeitlichen Intervall Bursts ausgeführt werden sollen.

Der Wertebereich des Parameters ist 1min bis 9min.

Aktion bei Unterschreitung der Erfolgsschwelle nach Ablauf des Messintervalls

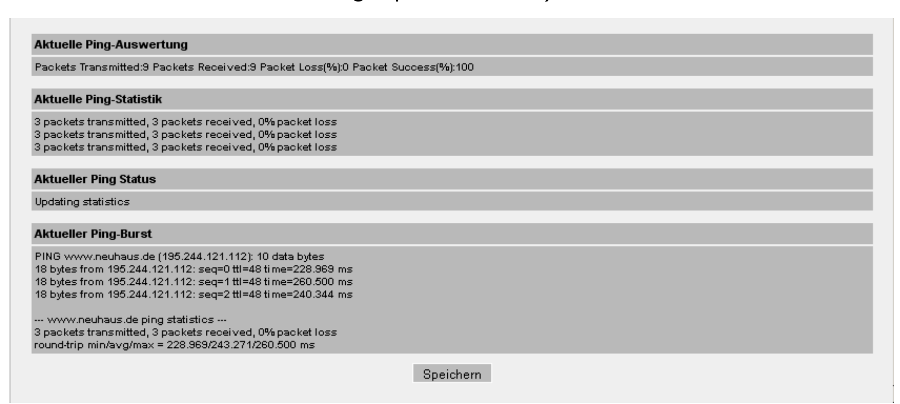
Verbindung erneuern	Das TAINY xMOD stellt erneut die Verbindung zum Datenfunkdienst (HSPA+, UMTS, EGPRS oder GPRS) her, falls die Ping-Erfolgsschwelle nicht erreicht wurde.
Neustart des Gerätes	Das TAINY xMOD führt einen Neustart durch, falls die Ping-Erfolgsschwelle nicht erreicht wurde.

Anderes Profil aktivieren	Das TAINY xMOD lädt ein anderes Profil, falls die Ping-Erfolgsschwelle nicht erreicht wurde, und versucht sich über dieses ins Netz eines Datenfunkdienstes einzuwählen. Das zu aktivierende Profil kann festgelegt werden, sobald die Aktion *Anderes Profil aktivieren* ausgewählt wurde.

Zuletzt aktiviertes Profil	default
Zu aktivierendes Profil	NONE

Zuletzt aktiviertes Profil	Zeigt den Namen des zuletzt im TAINY xMOD aktivierten Konfigurationsprofils an.
Zu aktivierendes Profil	Legen Sie hier das Profil fest, zu dem gewechselt wird, sollte die Verbindungsprüfung fehlschlagen (Es können nur Profile gewählt werden, die bereits im Gerät abgespeichert sind).

Statistik



Im Modus *Statistik* gibt die Webseite verschiedene Statistikwerte des aktuell laufenden Messintervalls aus. Das obige Beispiel zeigt die Daten einer Verbindungsprüfung nach drei Bursts mit je drei abgesetzten Ping-Kommandos. Alle Ping-Kommandos wurden erfolgreich beantwortet.

Nach Ablauf des Messintervalls werden die Daten ausgewertet und aus der Anzeige gelöscht.

Aktuelle Ping-Auswertung	Zeigt die Auswertung aller bisher im aktuellen Messintervall durchgeführten Ping-Tests an. Das hier errechnete Ergebnis (*Packet Success*) wird am Ende des Messintervalls mit der *Ping-Erfolgsschwelle* verglichen.
Aktuelle Ping-Statistik	Listet die Auswertung aller bisher im aktuellen Messintervall durchgeführten Ping-Bursts einzeln auf.
Aktueller Ping-Status	Zeigt den aktuellen Status des Ping-Tests an.
Aktueller Ping-Burst	Listet die Auswertung der im letzten Ping-Burst abgesetzten Ping-Kommandos inklusive der Paketumlaufzeit auf.

Werkseinstellung

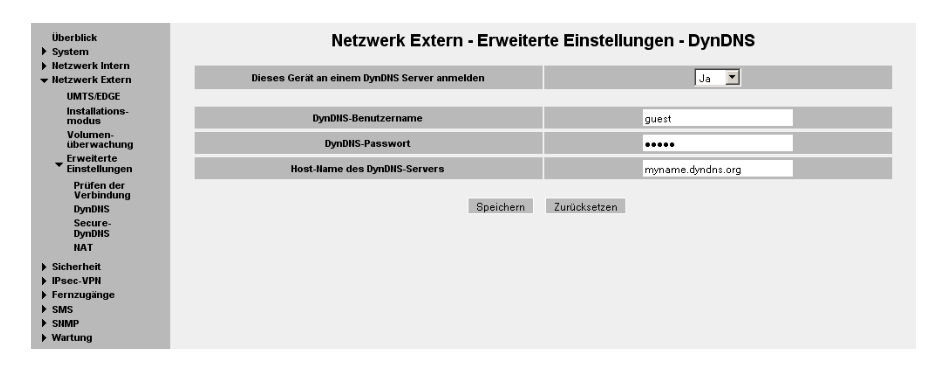
Werkseitig hat das TAINY xMOD folgende Einstellungen:

Prüfen der Verbindung	**Nein (Ausgeschaltet)**
Ziel-Hostname oder IP-Adresse der Ping-Gegenstelle	**NONE (leer)**
Maximale Ping-Erfolgsschwelle (5%-100%)	**80**
Anzahl der Daten-Bytes in einem Ping-Paket (0-65535)	**10**
Maximale Wartezeit auf eine Ping-	**30**

Antwort (1-60) Sekunden	
Länge des Messintervalls (10-30) Minuten	**10**
Anzahl der einzelnen Pings pro Ping-Burst (1-20)	**10**
Zeitabstand zwischen den Ping-Bursts pro Messintervall (1-9) Minuten	**1**
Aktion bei fehlerhafter Verbindung	**Verbindung erneuern**
Zu aktivierendes Profil	**NONE**

5.3 Host-Name durch DynDNS

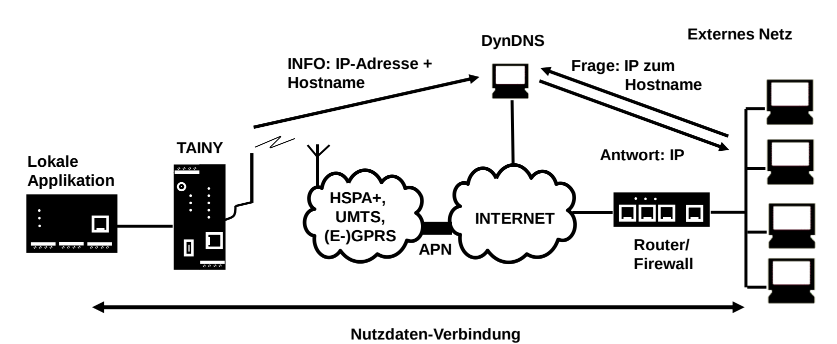
Netzwerk Extern > Erweiterte Einstellungen > DynDNS



Funktion

Dynamische Domain Name Server (DynDNS) ermöglichen es Applikationen im Internet, unter einem Host-Namen (z.B. myHost.org) erreichbar zu sein, auch wenn diese Applikationen keine feste IP-Adresse haben und der Host-Name nicht registriert ist. Wenn Sie das TAINY xMOD bei einem DynDNS-Dienst anmelden, können Sie das TAINY xMOD aus dem externen Netz auch unter einem Host-Namen erreichen, z.B. myTainy.dyndns.org. Das TAINY xMOD ist kompatibel zu **dyndns.org**.

Weitere Informationen zu DynDNS finden Sie im Kapitel 16.



Hinweis: HSPA+ und UMTS werden nur vom TAINY HMOD unterstützt.

Dieses Gerät an einem DynDNS-Server anmelden

Wählen Sie *Ja,* wenn Sie einen DynDNS-Dienst verwenden wollen.

DynDNS-Benutzername / -Passwort

Geben Sie hier den Benutzernamen und das Passwort ein, das Sie zur Nutzung des DynDNS-Service berechtigt. Ihr DynDNS-Anbieter teilt Ihnen diese Angaben mit.

DynDNS Host-Name

Geben Sie hier den Host-Namen ein, den Sie für das TAINY xMOD mit Ihrem DynDNS-Anbieter vereinbart haben, z.B. myTAINY.dyndns.org.

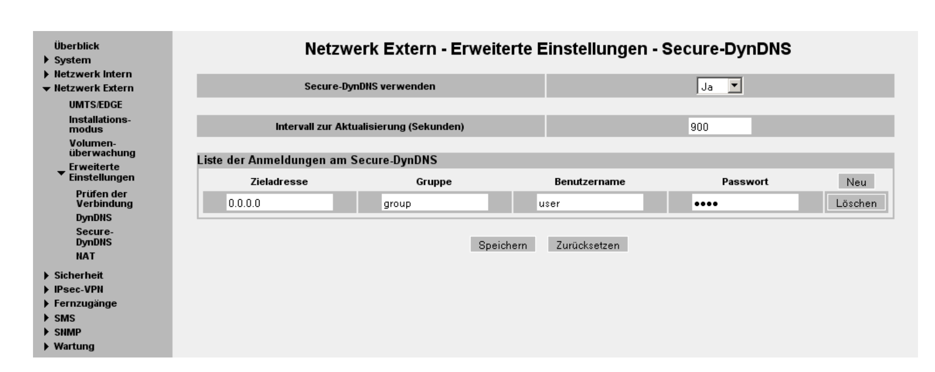
Werkseinstellung

Werkseitig hat TAINY xMOD folgende Einstellungen:

Das Gerät an einem DynDNS-Server anmelden	**Nein (Ausgeschaltet)**
DynDNS-Benutzername	**guest**
DynDNS-Passwort	**guest**
Host-Name des DynDNS-Servers	**myname.dyndns.org**

5.4 Secure-DynDNS

Netzwerk Extern > Erweiterte Einstellungen > Secure-DynDNS



Funktion

Bei aktivierter Secure-DynDNS-Funktion übermittelt das TAINY xMOD seine vom Datenfunkdienst zugewiesene externe IP-Adresse per gesichertem https-Protokoll an einen einstellbaren Zielserver.

Das Verfahren ist vergleichbar mit dem DynDNS-Dienst und erfordert einen entsprechenden Zugang auf der Serverseite.

Secure-DynDNS verwenden

Wählen Sie *Ja*, wenn Sie die Secure-DynDNS-Funktion aktivieren möchten.

Mit *Neu* können Sie weitere Zielserver hinzufügen, mit *Löschen* bestehende Einträge entfernen.

Intervall zur Aktualisierung (Sekunden)

Geben Sie hier das Intervall in Sekunden an, mit dem die zugewiesene IP-Adresse des TAINY xMOD an den eingestellten Zielserver übertragen werden soll.

Liste der Anmeldungen am Secure-DynDNS

Geben Sie hier die Zieladresse und die Zugangsdaten von einem oder mehreren Zielservern an:

Zieladresse

Geben Sie hier die IP-Adresse des Zielservers an.

Gruppe

Geben Sie hier die Gruppen-Information ein.

Benutzername

Geben Sie hier den Benutzernamen für den Zugang am Zielserver ein.

Passwort

Geben Sie hier das Passwort für den Zugang am Zielserver ein.

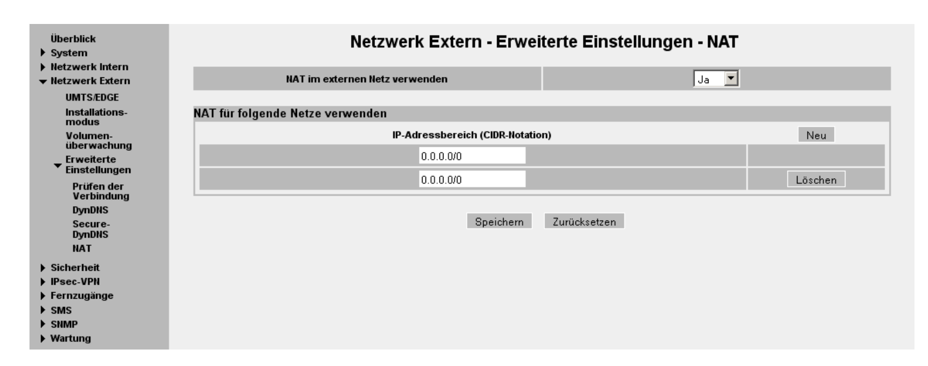
Werkseinstellung

Werkseitig hat TAINY xMOD folgende Einstellungen:

Secure-DynDNS verwenden	**Nein (Ausgeschaltet)**
Intervall zur Aktualisierung	**900 Sekunden**
Zieladresse	**0.0.0.0**
Gruppe	**group**
Benutzername	**user**
Passwort	**pass**

5.5 NAT – Network Address Translation

Netzwerk Extern > Erweiterte Einstellungen > NAT



Funktion

Listet die festgelegten Regeln für NAT (**N**etwork **A**ddress **T**ranslation) auf und ermöglicht, Regeln zu setzen oder zu löschen.

Das Gerät kann bei ausgehenden Datenpaketen die angegebenen Absender-IP-Adressen aus seinem internen Netzwerk auf seine eigene externe Adresse umschreiben, eine Technik, die als NAT (Network Address Translation) bezeichnet wird.

Diese Methode wird benutzt, wenn die internen Adressen extern nicht geroutet werden können oder sollen, z. B. weil ein privater Adressbereich wie 192.168.x.x benutzt wird oder weil die interne Netzstruktur verborgen werden soll.

Dieses Verfahren wird auch *IP-Masquerading* genannt.

NAT im externen Netz verwenden

Wählen Sie *Ja*, um die NAT-Funktion zum externen Netz zu aktivieren.

NAT für folgende Netze verwenden

Geben Sie die Netzwerke an, für die NAT genutzt werden soll. Die Angabe erfolgt als Adressbereich. Verwenden Sie die CIDR-Syntax

Neu – Netzwerk hinzufügen

Löschen – Netzwerk löschen

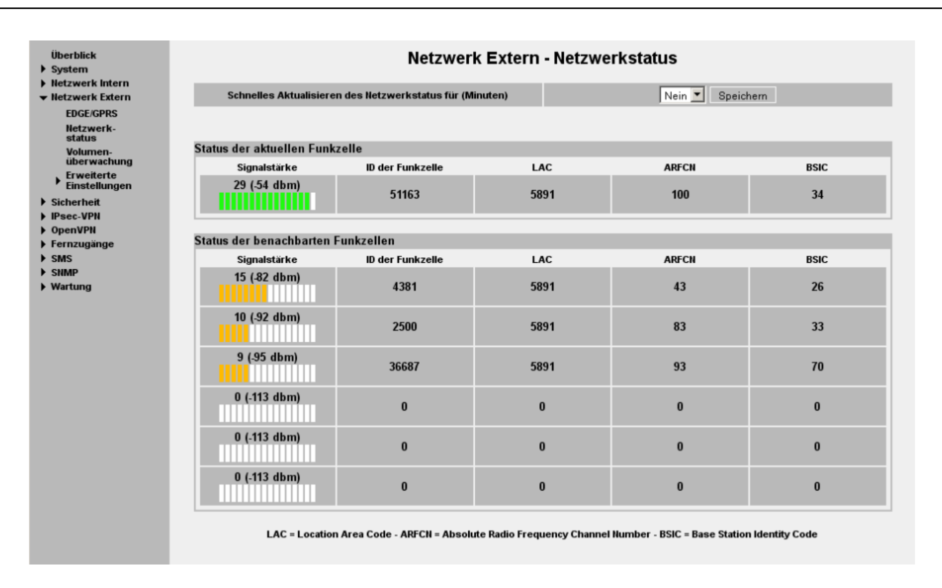
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

NAT im externen Netz verwenden	**Ja (Eingeschaltet)**
IP-Adressbereich (CIDR-Notation)	**0.0.0.0/0**.

5.6 Netzwerkstatus

Netzwerk Extern > Netzwerkstatus



Die Seite *Netzwerkstatus* enthält Informationen über die aktuell verwendete Funkzelle sowie sichtbare Funkzellen in der Umgebung des TAINY xMOD.

Im Normalbetrieb werden die in *Netzwerkstatus* angezeigten Signalstärken und Kenndaten der Funkzellen alle 60s aktualisiert. Um das Positionieren der Antenne(n) zu unterstützen, kann darüber hinaus der Modus *Schnelles Aktualisieren des Netzwerkstatus* aktiviert werden. In diesem Modus aktualisiert das TAINY xMOD die hier angezeigten Werte sowie die Anzeige der Signalleuchte Q (Quality) ca. alle 3s.

Die Position der Antenne sollte dabei solange verändert werden, bis das angezeigte Signal der aktuellen Zelle ein Maximum erreicht hat.

Unabhängig vom eingestellten Modus, d.h. der Aktualität der Werte, aktualisiert sich die Webseite ca. alle 3s.

Schnelles Aktualisieren des Netzwerkstatus für (Minuten)
: Zum Aktivieren des Modus S*chnelles Aktualisieren des Netzwerkstatus* wählen Sie einen der vorgegebenen Minutenwerte und übernehmen diesen mit *Speichern*. Nach Ablauf der eingestellten Zeitspanne wird das *schnelle Aktualisieren* automatisch beendet und das Gerät wechselt zurück in den Normalbetrieb.

Wählen Sie *Nein*, um das schnelle Aktualisieren zu beenden und zum Normalbetrieb zurückzukehren.

5.6.1 Netzwerkstatus im 2G-Betrieb (TAINY EMOD)

Status der aktuellen Funkzelle

Signalstärke	ID der Funkzelle	LAC	ARFCN	BSIC
29 (-54 dbm)	51163	5891	100	34

Status der benachbarten Funkzellen

Signalstärke	ID der Funkzelle	LAC	ARFCN	BSIC
15 (-82 dbm)	4381	5891	43	26
10 (-92 dbm)	2500	5891	83	33
9 (-95 dbm)	36687	5891	93	70
0 (-113 dbm)	0	0	0	0
0 (-113 dbm)	0	0	0	0
0 (-113 dbm)	0	0	0	0

LAC = Location Area Code - ARFCN = Absolute Radio Frequency Channel Number - BSIC = Base Station Identity Code

Status der aktuellen Funkzelle
: Zeigt die Kenndaten der Funkzelle an, mit der das TAINY xMOD aktuell verbunden ist.

Status der benach-barten Funkzellen
: Zeigt die Kenndaten benachbarter Funkzellen an, von denen das TAINY xMOD Signale empfängt.

Signalstärke
: Anzeige der Qualität/Feldstärke, mit der das Signal der Funkzelle empfan-gen wird, angegeben als CSQ- und als RSSI-Wert [dBm].

ID der Funkzelle
: Gibt die Kennung (Cell-ID) der Funkzelle an.

LAC
: Gibt die Kennung (LAC) des aus mehreren Basisstationen/Funkzellen bestehenden Netzabschnittes in der Umgebung des TAINY xMOD an.

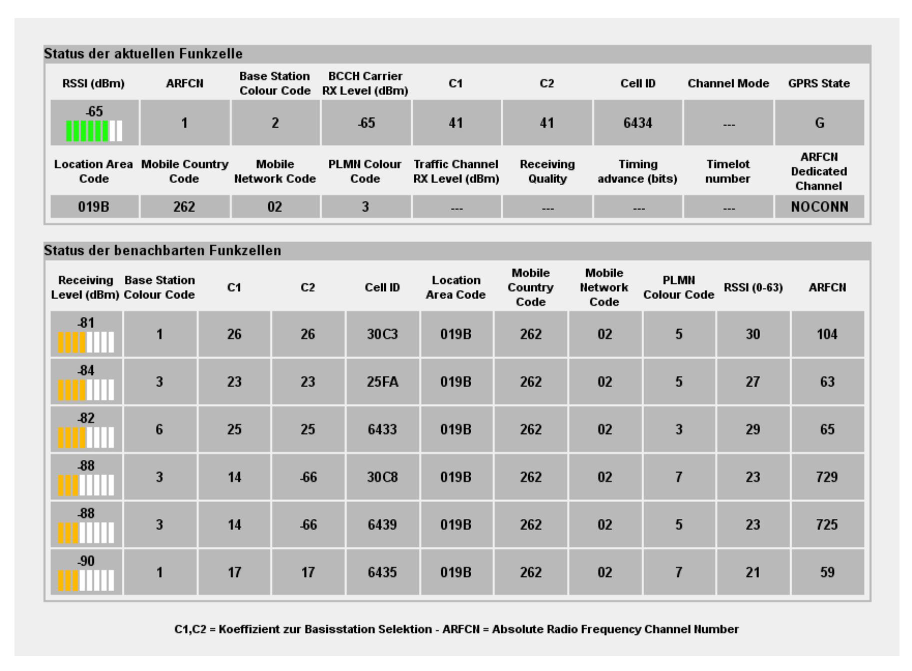
ARFCN
: Gibt die absolute Kanalnummer (ARFCN) des Funkkanals an, auf dem die Funkzelle sendet.

BSIC
: Gibt die Kennung (BSIC) der Basisstation an, zu der die Funkzelle gehört.

Werkseinstellung
: Werkseitig hat das TAINY xMOD folgende Einstellungen:

Schnelles Aktualisieren des Netzwerkstatus für (Minuten)	**Nein (Ausgeschaltet)**

5.6.2 Netzwerkstatus im 2G-Betrieb (TAINY HMOD)



Status der aktuellen Funkzelle

RSSI (dBm)	ARFCN	Base Station Colour Code	BCCH Carrier RX Level (dBm)	C1	C2	Cell ID	Channel Mode	GPRS State
-65	1	2	-65	41	41	6434	---	G

Location Area Code	Mobile Country Code	Mobile Network Code	PLMN Colour Code	Traffic Channel RX Level (dBm)	Receiving Quality	Timing advance (bits)	Timelot number	ARFCN Dedicated Channel
019B	262	02	3	---	---	---	---	NOCONN

Status der benachbarten Funkzellen

Receiving Level (dBm)	Base Station Colour Code	C1	C2	Cell ID	Location Area Code	Mobile Country Code	Mobile Network Code	PLMN Colour Code	RSSI (0-63)	ARFCN
-81	1	26	26	30C3	019B	262	02	5	30	104
-84	3	23	23	25FA	019B	262	02	5	27	63
-82	6	25	25	6433	019B	262	02	3	29	65
-88	3	14	-66	30C8	019B	262	02	7	23	729
-88	3	14	-66	6439	019B	262	02	5	23	725
-90	1	17	17	6435	019B	262	02	7	21	59

C1,C2 = Koeffizient zur Basisstation Selektion - ARFCN = Absolute Radio Frequency Channel Number

Status der aktuellen Funkzelle	Zeigt die Kenndaten der Funkzelle an, mit der das TAINY xMOD aktuell verbunden ist.
RSSI (dBm)	Zeigt die Empfangsfeldstärke auf dem Kanal der aktuell verwendeten Funkzelle an.
ARFCN	Gibt die absolute Kanalnummer des Funkkanals an, auf dem die Funkzelle sendet.
Base Station Colour Code	Gibt die Kennung der aktuellen Basisstation (Colour Code) an.
BCCH Carrier RX Level (dBm)	Gibt den Empfangspegel auf der Trägerfrequenz des BCCH (Broadcast Control Channel) an.
C1	Gibt den ersten Koeffizienten für die Auswahl einer Basisstation an.
C2	Gibt den zweiten Koeffizienten für die Auswahl einer Basisstation an.
Cell ID	Gibt die Kennung der aktuellen Funkzelle an.
Channel Mode	Gibt an, in welchem Modus der dedizierte Kanal arbeitet.
GPRS State	Zeigt den Status der GPRS-Verbindung an.
Location Area Code	Gibt die Kennung (LAC) des aus mehreren Basisstationen/Funkzellen bestehenden Netzabschnittes in der Umgebung des TAINY xMOD an.
Mobile Country Code	Gibt die Länderkennung (MCC) des verwendeten Mobilfunk-Providers an.
Mobile Network Code	Gibt die Netzkennung (MNC) des verwendeten Mobilfunk-Providers an.
PLMN Colour Code	Gibt die Kennung (Colour Code) des Mobilfunk-Providers an, der die Basisstation der aktuell verwendeten Funkzelle betreibt.
Traffic Channel RX Level (dBm)	Gibt den Empfangspegel des Datenkanals in dBm an.
Receiving Quality	Zeigt die Empfangsqualität des dedizierten Kanals (0-7).
Timing advance (bits)	Gibt den Zeitvorlauf in Bits an (dedizierter Kanal).

Timeslot number	Gibt die Nummer des aktuell zugewiesenen Zeitschlitzes an.
ARFCN Dedicated Channel	Gibt die absolute Kanalnummer des dedizierten Kanals an.
Status der benachbar-ten Funkzellen	Zeigt die Kenndaten benachbarter Funkzellen an, von denen das TAINY xMOD Signale empfängt.
Receiving Level (dBm)	Gibt den Empfangspegel der Nachbarzelle in dBm an.
Base Station Colour Code	Gibt die Kennung der zur Nachbarzelle gehörenden Basisstation (Colour Code) an.
C1	Gibt den ersten Koeffizienten für die Auswahl einer Basisstation an (benachbarte Funkzelle).
C2	Gibt den zweiten Koeffizienten für die Auswahl einer Basisstation an (benachbarte Funkzelle).
Cell ID	Gibt die Kennung der benachbarten Funkzelle an.
Location Area Code	Gibt die Kennung (LAC) des aus mehreren Basisstationen/Funkzellen bestehenden Netzabschnittes in der Umgebung des TAINY xMOD an.
Mobile Country Code	Gibt die Länderkennung (MCC) des Mobilfunk-Providers der benachbar-ten Funkzelle an.
Mobile Network Code	Gibt die Netzkennung (MNC) des Mobilfunk-Providers der benachbarten Funkzelle an.
PLMN Colour Code	Gibt die Kennung (Colour Code) des Mobilfunk-Providers an, der die Basisstation der benachbarten Zelle betreibt.
RSSI (0-63)	Zeigt die Empfangsfeldstärke auf dem Kanal der benachbarten Funkzelle an.
ARFCN	Gibt die absolute Kanalnummer des Funkkanals an, auf dem die Nachbar-zelle sendet.

Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Schnelles Aktualisieren des Netzwerkstatus für (Minuten)	**Nein (Ausgeschaltet)**

5.6.3 Netzwerkstatus im 3G-Betrieb

Status der aktuellen Funkzelle

Cell ID	Compressed Mode	Ec/Io (dB) Control Channel	Ec/Io (dB) Dedicated Channel	HSDPA Typ	HSUPA Typ	Location Area Code	Mobile Country Code	Mobile Network Code
2636434	---	-24.0	---	---	---	0579	262	02
Physical Channel Type	**Primary Scrambling Code**	**RSCP (dBm) Control Channel**	**RSCP (dBm) Dedicated Channel**	**Spreading Factor**	**Slot Format**	**Cell Selection Quality (dB)**	**Cell Selection RX Level (dB)**	**UARFNC**
NOCONN	238	-121	---	---	---	23	22	10564

Status der benachbarten Funkzellen

Ec/Io (dB)	Primary Scrambling Code	RSCP (dBm)	Cell Selection Quality (dB)	Cell Selection RX Level (dB)	UARFCN
-5.5	238	-94	25	20	10564
-14.5	485	-103	7	11	10564
-24.0	189	-115	-16	-1	10564
-24.0	201	-120	-27	-6	10564
-24.0	52	-116	-19	-2	10564
-24.0	230	-115	-17	-1	10564

RSCP = Received Signal Code Power - UARFCN = UTRAN Absolute Radio Frequency Channel Number

Status der aktuellen Funkzelle	Zeigt die Kenndaten der Funkzelle an, mit der das TAINY xMOD aktuell verbunden ist.
Cell ID	Gibt die Kennung der Funkzelle an.
Compressed Mode	Zeigt an, ob das Gerät im Compressed Mode arbeitet.
Ec/Io (dB) Control Channel	Gibt den Signal-Rausch-Abstand des Kontrollkanals an.
Ec/Io (dB) Dedicated Channel	Gibt den Signal-Rausch-Abstand des Datenkanals an.
HSDPA Typ	Gibt den High-Speed-Download-Packet-Access-Typ an. Dieser Parameter wird nicht von allen Mobilfunk-Providern übermittelt.
HSUPA Typ	Gibt den High-Speed-Upload-Packet-Access-Typ an. Dieser Parameter wird nicht von allen Mobilfunk-Providern übermittelt.
Location Area Code	Gibt die Kennung (LAC) des aus mehreren Basisstationen/Funkzellen bestehenden Netzabschnittes in der Umgebung des TAINY xMOD an.
Mobile Country Code	Gibt die Länderkennung (MCC) des verwendeten Mobilfunk-Providers an.
Mobile Network Code	Gibt die Netzkennung (MNC) des verwendeten Mobilfunk-Providers an.
Physical Channel Type	Gibt den Typ des physikalischen Übertragungskanals an.
Primary Scrambling Code	Gibt den individuellen Verschlüsselungscode an, mit dem Datenpakete eindeutig der verwendeten Basisstation/Funkzelle zugeordnet werden können.
RSCP (dBm) Control Channel	Gibt die demodulierte Kanalleistung des Kontrollkanals an.
RSCP (dBm) Dedicated Channel	Gibt die demodulierte Kanalleistung des Datenkanals an.
Spreading Factor	Gibt die Größe des Spreizfaktors für die Datenübertragung über das UMTS-Netz an.
Slot Format	Gibt das Slot-Format des physikalischen Übertragungskanals an.
Cell Selection Quality	Gibt den Wert *Cell Selection Quality* an, der neben anderen zur Auswahl

(dB)	der zu verwendenden Funkzelle benutzt wird.
Cell Selection Rx Level (dB)	Gibt den Wert *Cell Selection Rx Level* an, der neben anderen zur Auswahl der zu verwendenden Funkzelle benutzt wird.
UARFCN	Gibt die absolute Kanalnummer (UARFCN) des Funkkanals an, auf dem die Funkzelle sendet.
Status der benach-barten Funkzellen	Zeigt die Kenndaten benachbarter Funkzellen an, von denen das TAINY xMOD Signale empfängt.
Ec/Io (dB)	Gibt den Signal-Rausch-Abstand des Kanals der Nachbarzelle an.
Primary Scrambling Code	Gibt den individuellen Verschlüsselungscode der Nachbarzelle an, mit dem Datenpakete eindeutig der verwendeten Basisstation/Funkzelle zugeordnet werden können.
RSCP (dBm)	Gibt die demodulierte Kanalleistung der Nachbarzelle an.
Cell Selection Quality (dB)	Gibt den Wert *Cell Selection Quality* der Nachbarzelle an.
Cell Selection Rx Level (dB)	Gibt den Wert *Cell Selection Rx Level* der Nachbarzelle an.
UARFCN	Gibt die absolute Kanalnummer (UARFCN) des Funkkanals an, auf dem die Nachbarzelle sendet.

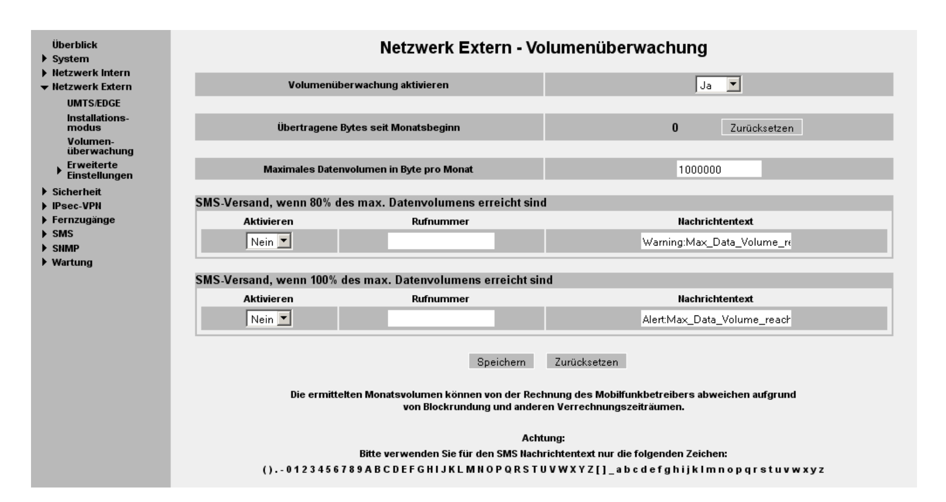
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Schnelles Aktualisieren des Netzwerkstatus für (Minuten)	**Nein (Ausgeschaltet)**

5.7 Volumenüberwachung

Netzwerk Extern – Volumen-überwachung



Überschreitet die Menge der vom TAINY xMOD gesendeten und empfangenen Daten das mit dem Mobilfunkbetreiber vereinbarte Datenvolumen, kann dies zu erheblichen Mehrkosten führen.

Daher kann es nützlich sein, wenn das TAINY xMOD das genutzte Datenvolumen ständig überwacht und bei drohender Überschreitung eines einstellbaren Grenzwertes eine Warnung versendet.

Hinweis

Das ermittelte Datenvolumen dient nur als Anhaltspunkt und kann von der Abrechnung des GSM-Netzbetreibers abweichen.

Volumenüberwachung	Wählen Sie *Ja*, um die Volumenüberwachung einzuschalten.

aktivieren	Wählen Sie *Nein*, um die Volumenüberwachung auszuschalten.
Übertragene Bytes seit Monatsbeginn	Zeigt die Anzahl der gesendeten und empfangenen Bytes seit Monatsbeginn an. **Hinweis** Setzen Sie manuell die Systemzeit des TAINY xMOD oder aktivieren Sie die NTP-Synchronisation, siehe Kapitel 4.7.
Zurücksetzen	Betätigen Sie die Schaltfläche, wenn Sie den Zähler für die gesendeten und empfangenen Bytes auf 0 zurücksetzen wollen. Zum Monatswechsel geschieht dies automatisch.
Maximales Datenvolumen in Byte pro Monat	Tragen Sie hier den Grenzwert für das monatliche Datenvolumen in Byte ein.
SMS-Versand, wenn 80% des max. Datenvolumens erreicht sind	Setzen Sie *Aktivieren* auf *Ja*, wenn das TAINY xMOD bei Erreichen von 80% des maximalen Datenvolumens eine SMS mit Warnmeldung an die angegebene Rufnummer versenden soll. Mit *Nein* wird der SMS-Versand deaktiviert.
SMS-Versand, wenn 100% des max. Datenvolumens erreicht sind	Setzen Sie *Aktivieren* auf *Ja*, wenn das TAINY xMOD bei Erreichen des maximalen Datenvolumens eine SMS mit Alarmmeldung an die angegebene Rufnummer versenden soll. Mit *Nein* wird der SMS-Versand deaktiviert.
Rufnummer	Geben Sie hier die Mobilfunkrufnummer an, an die die SMS mit Alarm- oder Warnmeldung gesendet werden soll.
Nachrichtentext	Geben Sie hier den Text der Alarm- bzw. Warn-SMS ein.
Zeichensatz	Bitte verwenden Sie für den SMS-Nachrichtentext nur diese Zeichen: , * ' # % = < > ! & + - / ? ( ) . : ; 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z (+ Leerzeichen)

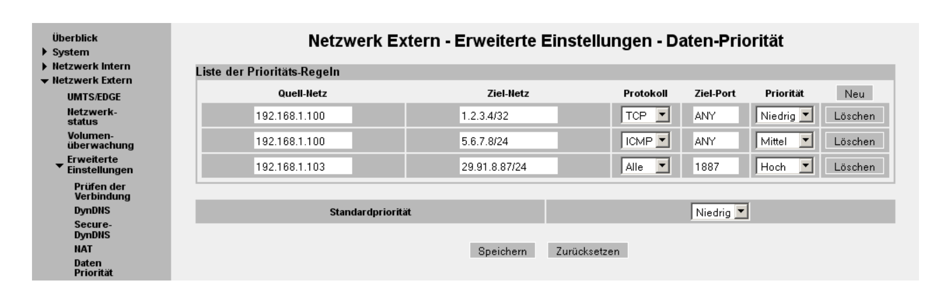
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Volumenüberwachung aktivieren	**Nein (Ausgeschaltet)**
Maximales Datenvolumen in Byte pro Monat	**1000000**
SMS-Versand, wenn 80% des max. Datenvolumens erreicht sind:	
Aktivieren	**Nein**
Rufnummer	**(leer)**
Nachrichtentext	**Warning:Max_Data_Volume_ reached**
SMS-Versand, wenn 100% des max. Datenvolumens erreicht sind:	
Aktivieren	**Nein**
Rufnummer	**(leer)**
Nachrichtentext	**Alert:Max_Data_Volume_ reached**

5.8 Daten-Priorität

Netzwerk Extern > Erweiterte Einstellungen > Daten-Priorität



Funktion

Mit dieser Funktion kann die Kommunikation für festgelegte Datenpfade priorisiert werden. Sind in einem Pfad mit der Priorität „Hoch“ Daten vorhanden, werden diese zuerst übertragen. Danach folgen Daten in Pfaden mit der Priorität „Mittel“. Nur wenn keine Daten in Pfaden hoher und mittlerer Priorität vorliegen, werden Daten in Pfaden mit Priorität „Niedrig“ übertragen.

Die Datenpfade werden über die IP-Adresse des Quell-Netzes und den IP-Adressbereich des Ziel-Netzes definiert. Zusätzlich kann ausgewählt werden auf welches Protokoll und auf welchen Ziel-Port sich die Priorisierung bezieht.

Mit *Neu* fügen Sie einen weiteren Datenpfad hinzu, mit *Löschen* entfernen Sie den Datenpfad aus der Liste.

Quell-Netz Tragen Sie den Quell-IP-Adressbereich des Datenpfads ein.

Ziel-Netz Tragen Sie den Ziel-IP-Adressbereich des Datenpfads ein.

Protokoll Geben Sie das Kommunikationsprotokoll an, das die gewählte Priorität bekommen soll.

Ziel-Port Tragen Sie den Ziel-Port des Datenpfads ein.

Priorität Legen Sie die Priorität des Datenpfads fest.

Standard-Priorität Legt die Priorität für jede Kommunikation fest, für die nicht explizit ein Datenpfad eingerichtet wurde.

Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Quell-Netz	**0.0.0.0/0**
Ziel-Netz	**0.0.0.0/0**
Protokoll	**Alle**
Ziel-Port	**ANY**
Priorität	**Niedrig**
Standard-Priorität	**Mittel**

6 Sicherheitsfunktionen

6.1 MAC-Filter

Sicherheit > MAC-Filter



Funktion

Das TAINY xMOD verfügt über einen MAC-Filter, der Kommunikation nur mit lokalen Applikationen zulässt, deren MAC-Adressen im TAINY xMOD eingetragen sind.

MAC-Filter aktivieren

Ja Der MAC-Filter ist eingeschaltet

Nein Der MAC-Filter ist ausgeschaltet

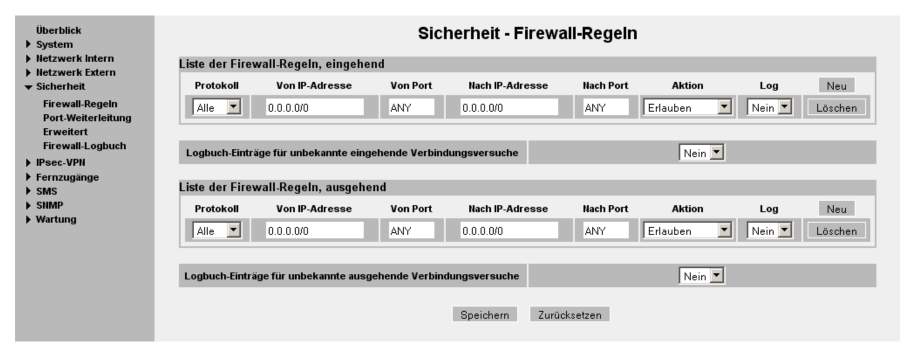
Liste der erlaubten MAC-Adressen

Geben Sie hier die MAC-Adressen der lokalen Applikationen ein, die mit dem / über das TAINY xMOD kommunizieren dürfen.

Fügen Sie mit *Neu* weitere MAC-Adressen ein bzw. entfernen Sie MAC-Adressen mit *Löschen*

6.2 Paketfilter

Sicherheit > Firewall-Regeln



Funktion

Das TAINY xMOD beinhaltet eine Stateful Inspection Firewall.

Stateful Inspection Firewall ist eine Methode zur Paketfilterung. Paketfilter lassen IP-Pakete nur dann passieren, wenn dies zuvor durch Firewall-Regeln definiert wurde. In der Firewall-Regel wird folgendes festgelegt,

- welches Protokoll (TCP, UDP, ICMP) passieren darf,
- die erlaubte Quelle der IP-Pakete (Von IP / Von Port)
- das erlaubte Ziel der IP-Pakete (Nach IP / Nach Port)

Gleichfalls wird hier festgelegt, wie mit IP-Pakete verfahren wird, die nicht passieren dürfen (verwerfen, zurückweisen).

Bei einem einfachen Paketfilter müssen immer zwei Firewall-Regeln für eine Verbindung angelegt werden:

- Eine Regel für die Anfragerichtung von der Quelle zum Ziel und
- eine zweite Regel für die Antwortrichtung vom Ziel zur Quelle.

Anders beim TAINY xMOD mit Stateful Inspection Firewall. Hier wird nur für die Anfragerichtung von der Quelle zum Ziel eine Firewall-Regel angelegt. Die Firewall-Regel für die Antwortrichtung vom Ziel zur Quelle ergibt sich aus der Analyse der zuvor gesendeten Daten. Die Firewall-Regel für die Antworten wird nach Erhalt der Antworten bzw. nach Ablauf einer kurzen Zeitspanne wieder geschlossen. Antworten dürfen also nur passieren, wenn es zuvor eine Anfrage gab. So kann die Antwortregel nicht für unbefugte Zugriffe benutzt werden. Besondere Verfahren ermöglichen zudem, dass auch UDP- und ICMP-Daten passieren können, obwohl diese Daten zuvor nicht angefordert wurden.

Liste der Firewall-Regeln, eingehend

Mit den Firewall-Regeln für eingehende Verbindungen wird festgelegt, wie mit IP-Paketen zu verfahren ist, die über den Datenfunkdienst (HSPA+, UMTS, EGPRS oder GPRS) aus externen Netzen (z.B. Internet) empfangen werden. Quelle ist der Absender dieser IP-Pakete. Ziel sind die lokalen Applikationen am TAINY xMOD.

Entsprechend der Werkseinstellung ist zunächst keine eingehende Firewall-Regel gesetzt, d.h. es dürfen keine IP-Pakete passieren.

Neu — Fügt eine weitere Firewall-Regel hinzu, die Sie dann ausfüllen können.

Löschen — Entfernt angelegte Firewall-Regeln wieder.

Protokoll — Wählen Sie das Protokoll aus, für das diese Regel gelten soll. Zur Auswahl stehen *TCP, UDP, ICMP*. Wenn Sie *Alle* wählen, gilt die Regel für alle drei Protokolle.

Hinweis

Wird für Protokoll *Alle* oder *ICMP* gewählt ist eine Portzuordnung nicht wirksam.

Von IP-Adresse — Tragen Sie die IP-Adresse der externen Gegenstelle ein, die IP-Pakete zum lokalen Netz senden darf. Geben Sie dazu die IP-Adresse oder einen IP-Bereich der Gegenstelle an. ***0.0.0.0/0*** bedeutet alle Adressen.

Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 16.

Von Port — Tragen Sie den Port (z.B. 80) oder Portbereich (z.B. 8080:9090) ein, von dem die externe Gegenstelle IP-Pakete senden darf.

(wird nur ausgewertet bei den Protokollen TCP und UDP)

Nach IP-Adresse — Tragen Sie ein, an welche IP-Adresse im lokalen Netz IP-Pakete gesendet werden dürfen. Geben Sie dazu die IP-Adresse oder einen IP-Bereich der Applikation im lokalen Netz an. ***0.0.0.0/0*** bedeutet alle Adressen.

Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 16.

Nach Port — Tragen Sie den Port (z.B. 80) oder Portbereich (z.B. 8080:9090) ein, an den die externe Gegenstelle IP-Pakete senden darf.

Aktion Wählen Sie aus, wie mit eintreffenden IP-Paketen zu verfahren ist:

Erlauben – Die Datenpakete dürfen passieren,

Zurückweisen – Die Datenpakete werden abgewiesen, der Absender erhält eine entsprechende Meldung,

Verwerfen – Die Datenpakete werden ohne Rückmeldung an den Absender verworfen.

Liste der Firewall-Regeln, ausgehend

Mit den Firewall-Regeln für ausgehende Verbindungen wird festgelegt, wie mit IP-Paketen zu verfahren ist, die vom lokaken Netz empfangen werden. Quelle ist eine Applikationen im lokalen Netz. Ziel ist eine externe Gegenstelle z.B. im Internet oder in einem privaten Netz.

Entsprechend der Werkseinstellung ist zunächst keine ausgehende Firewall-Regel gesetzt, d.h. es dürfen keine IP-Pakete passieren.

Neu Fügt eine weitere Firewall-Regel hinzu, die Sie dann ausfüllen können.

Protokoll Wählen Sie das Protokoll aus, für das diese Regel gelten soll. Zur Auswahl stehen *TCP, UDP, ICMP*. Wenn Sie *Alle* wählen, gilt die Regel für alle drei Protokolle.

Von IP-Adresse Tragen Sie die IP-Adresse der lokalen Applikation ein, die IP-Pakete zum externen Netz senden darf. Geben Sie dazu die IP-Adresse oder einen IP-Bereich der lokalen Applikation an. ***0.0.0.0/0*** bedeutet alle Adressen.

Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 16.

Von Port Tragen Sie den Port ein, von dem die lokale Applikation IP-Pakete senden darf. Geben Sie dazu die Portnummer an.

(wird nur ausgewertet bei den Protokollen TCP und UDP)

Nach IP-Adresse Tragen Sie ein, an welche IP-Adresse im externen Netz IP-Pakete gesendet werden darf. Geben Sie dazu die IP-Adresse oder einen IP-Bereich der Applikation im Netz an. ***0.0.0.0/0*** bedeutet alle Adressen.

Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 16.

Nach Port Tragen Sie ein, an welchen Port die lokale Applikation IP-Pakete senden darf. Geben Sie dazu die Portnummer an.

(wird nur ausgewertet bei den Protokollen TCP und UDP)

Aktion Wählen Sie aus, wie mit abgehenden IP-Paketen zu verfahren ist:

Erlauben – Die Datenpakete dürfen passieren,

Zurückweisen – Die Datenpakete werden abgewiesen, der Absender erhält eine entsprechende Meldung,

Verwerfen – Die Datenpakete werden ohne Rückmeldung an den Absender verworfen.

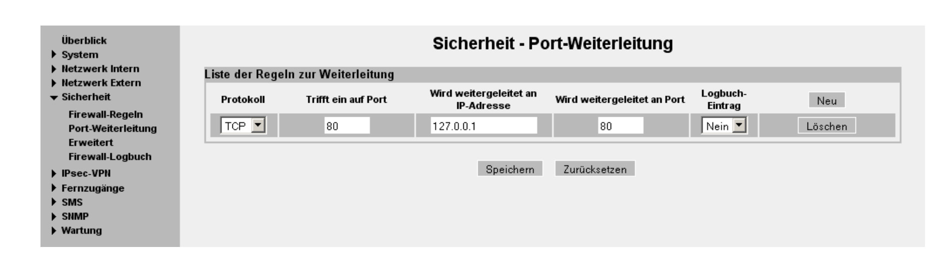
Firewall-Regeln Ein-/ Ausgehend	*Log*	Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel - das Ereignis protokolliert werden soll - *Log* auf *Ja* setzen - oder nicht - *Log* auf *Nein* setzen (werkseitige Voreinstellung) Das Protokoll wird in das Firewall-Logbuch, siehe Kapitel 6.5 geschrieben.
Log-Einträge für unbekannte Verbindungsversuche	Damit werden alle Verbindungsversuche protokolliert, die die festgelegten Regeln nicht erfassen. Diese Funktion kann separat für ausgehende und eingehende Verbindungsversuche eingestellt werden.	

Werkseinstellung Werkseitig hat das TAINY xMOD folgende Einstellungen:

Firewall eingehend	Liste der Firewall-Regeln, eingehend	**- (Alles gesperrt)**
	Protokoll	**Alle**
	Von IP-Adresse	**0.0.0.0/0**
	Von Port	**ANY**
	Nach IP-Adresse	**0.0.0.0/0**
	Nach Port	**ANY**
	Aktion	**Erlauben**
	Log	**Nein (Ausgeschaltet)**
	Log-Einträge für unbekannte eingehende Verbindungsversuche	**Nein (Ausgeschaltet)**
Firewall ausgehend	Liste der Firewall-Regeln, ausgehend	**- (Alles gesperrt)**
	Protokoll	**Alle**
	Von IP-Adresse	**0.0.0.0/0**
	Von Port	**ANY**
	Nach IP-Adresse	**0.0.0.0/0**
	Nach Port	**ANY**
	Aktion	**Erlauben**
	Log	**Nein (Ausgeschaltet)**
	Log-Einträge für unbekannte ausgehende Verbindungsversuche	**Nein (Ausgeschaltet)**

6.3 Port-Weiterleitung

Sicherheit > Port-Weiterleitung



Funktion

Ist eine Regel zur Port-Weiterleitung erstellt, dann werden Datenpakete, die aus dem externen Netz auf einem festgelegten IP-Port des TAINY xMOD eintreffen, an eine festgelegte IP-Adresse und Port-Nummer im lokalen Netz weitergeleitet. Die Port-Weiterleitung kann für TCP oder UDP konfiguriert werden.

Bei Port-Weiterleitung geschieht Folgendes: Der Header eingehender Datenpakete aus dem externen Netz, die an die externe IP-Adresse des TAINY xMOD sowie an einen bestimmten Port gerichtet sind, werden so umgeschrieben, dass sie ins interne Netz an einen bestimmten Rechner und zu einem bestimmten Port dieses Rechners weitergeleitet werden. D. h. die IP-Adresse und Port-Nummer im Header eingehender Datenpakete werden geändert.

Dieses Verfahren wird auch Destination-NAT oder Port Forwarding genannt.

Hinweis

Damit ankommende Datenpakete an die festgelegte IP-Adresse im lokalen Netz weitergeleitet werden können, muss für diese IP-Adresse eine entsprechende eingehende Firewall-Regel im Paketfilter eingerichtet werden. Siehe Kapitel 6.1.

Neu — Fügt eine neue Weiterleitungs-Regel hinzu, die Sie dann ausfüllen können.

Löschen — Entfernt angelegte Weiterleitungs-Regeln wieder.

Protokoll — Geben Sie hier das Protokoll (TCP oder UDP) an, auf das sich die Regel beziehen soll.

Trifft ein auf Port — Geben Sie hier die Portnummer (z.B. 80) an, auf dem die Datenpakete aus dem externen Netz eintreffen, die weitergeleitet werden sollen.

Wird weiter-geleitet an IP-Adresse — Geben Sie hier die IP-Adresse im lokalen Netz an, an die die eintreffenden Datenpakete weitergeleitet werden sollen.

Wird weiter-geleitet an Port — Geben Sie hier die Portnummer (z.B. 80) zur IP-Adresse im lokalen Netz an, an den die eintreffenden Datenpakete weitergeleitet werden sollen.

Logbuch-Eintrag — Für jede einzelne Port-Weiterleitungs-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf *Ja* setzen
- oder nicht - *Log* auf *Nein* setzen (Werkseinstellung).

Das Protokoll wird in das Firewall-Logbuch, siehe Kapitel 6.5 geschrieben.

Werkseinstellung

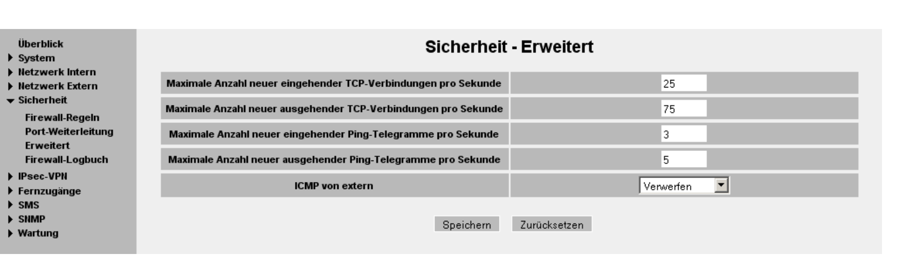
Werkseitig hat das TAINY xMOD folgende Einstellungen:

Regeln zur Weiterleitung	**-**
Protokoll	**TCP**
Trifft ein auf Port	**80**
Wird weitergeleitet an IP-Adresse	**127.0.0.1**
Wird weitergeleitet an Port	**80**

Logbuch-Eintrag	**Nein (Ausgeschaltet)**

6.4 Erweiterte Sicherheitsfunktionen

Sicherheit > Erweitert



Funktion

Die erweiterten Sicherheitsfunktionen dienen dazu, das TAINY xMOD und die lokalen Applikationen gegen Angriffe zu schützen. Zum Schutz wird angenommen, dass nur eine bestimmte Anzahl von Verbindungen oder empfangener Ping-Pakete im normalen Betrieb zulässig und erwünscht sind, und dass bei einer plötzlichen Häufung ein Angriff stattfindet.

Maximale Zahl …

Die Einträge

- Maximale Anzahl neuer eingehender TCP-Verbindungen pro Sekunde
- Maximale Anzahl neuer ausgehender TCP-Verbindungen pro Sekunde
- Maximale Anzahl neuer eingehender Ping-Telegramme pro Sekunde
- Maximale Anzahl neuer ausgehender Ping-Telegramme pro Sekunde

legen Obergrenzen fest. Die Voreinstellungen (siehe Abbildung) sind so gewählt, dass sie bei normalem praktischem Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte entsprechend ändern.

ICMP von extern

Mit dieser Option können Sie das Verhalten beim Empfang von ICMP-Paketen beeinflussen, die aus dem externen Netz in Richtung des TAINY xMOD gesendet werden. Sie haben folgende Möglichkeiten:

- *Verwerfen*: Alle ICMP-Pakete zum TAINY xMOD werden verworfen.
- *Ping erlauben*: Nur Ping-Pakete (ICMP Typ 8) zum TAINY xMOD werden akzeptiert.
- *Erlauben*: Alle Typen von ICMP-Pakete zum TAINY xMOD werden akzeptiert.

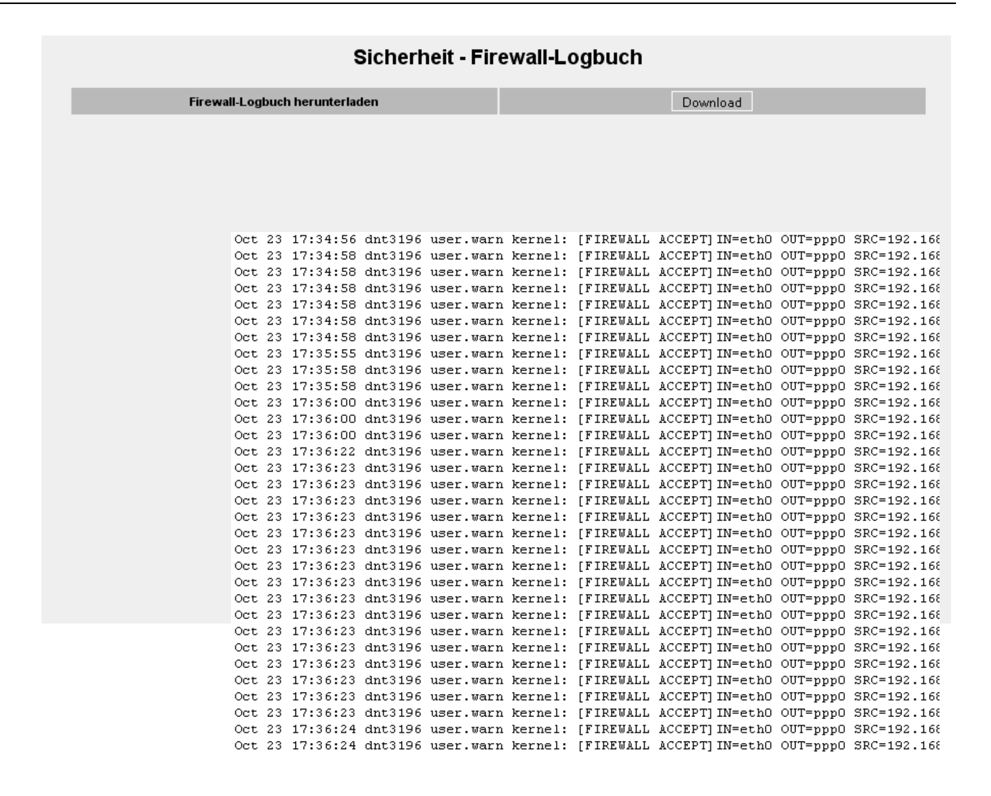
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Maximale Anzahl neuer eingehender TCP-Verbindungen pro Sekunde	**25**
Maximale Anzahl neuer ausgehender TCP-Verbindungen pro Sekunde	**75**
Maximale Anzahl neuer eingehender Ping-Telegramme pro Sekunde	**3**
Maximale Anzahl neuer ausgehender Ping-Telegramme pro Sekunde	**5**
ICMP von extern	**Verwerfen**

6.5 Firewall-Logbuch

Sicherheit > Firewall Logbuch



Funktion

Im Firewall-Logbuch wird eingetragen, wann einzelne Firewall-Regeln angewendet wurden. Dazu muss zu den verschiedenen Firewall-Funktionen die Log-Funktion aktiviert werden.

Achtung

Das Firewall-Logbuch geht bei einem Neustart verloren.

7 IPsec-VPN-Verbindungen

NUR TAINY xMOD-V3

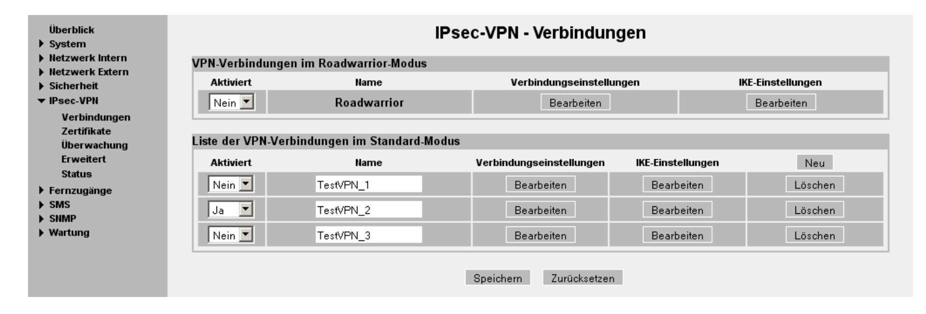
Hinweis zum Funktionsumfang

Der Menüpunkt IPsec-VPN findet sich nur beim TAINY xMOD-V3-Geräten. Nur TAINY xMOD-V3-Geräte unterstützen IPsec-VPN-Verbindungen.

7.1 Einleitung

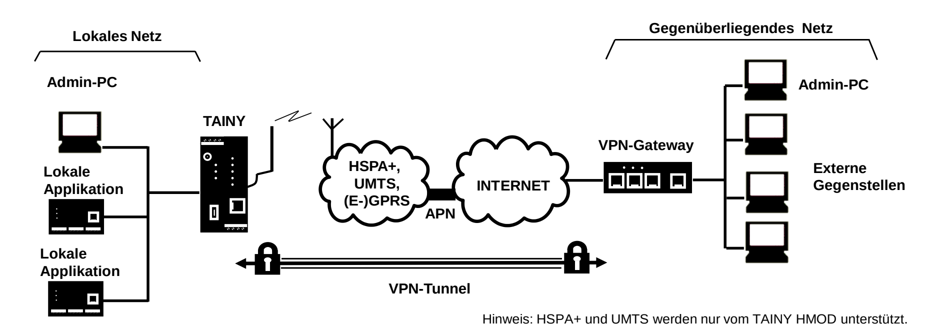
IPsec-VPN > Verbindungen

NUR TAINY xMOD-V3



Funktion

Das TAINY xMOD-V3 kann das lokale Netz über einen VPN-Tunnel mit einem befreundeten gegenüberliegenden Netz verbinden. Die IP-Datenpakete, die zwischen den beiden Netzen ausgetauscht werden, werden verschlüsselt und sind durch den VPN-Tunnel gegen unerlaubte Manipulationen geschützt. So können auch ungeschützte öffentliche Netze wie das Internet zum Transport der Daten verwendet werden, ohne die Vertraulichkeit oder Integrität der Daten zu gefährden.



Damit das TAINY xMOD-V3 einen VPN-Tunnel aufbauen kann, muss das gegenüberliegende Netz über ein VPN-Gateway als Gegenstation des TAINY xMOD-V3 verfügen.

Das TAINY xMOD-V3 verwendet für den VPN-Tunnel das IPsec-Verfahren im Tunnelmodus. Dabei werden die zu übertragenden IP-Datenpakete vollkommen verschlüsselt und mit einem neuen Header versehen, bevor sie zum VPN-Gateway der Gegenstelle gesendet werden. Dort werden die empfangenen Datapakete entschlüsselt und aus ihnen die ursprünglichen Datapakete wiederhergestellt. Diese werden dann zum Ziel im gegenüberliegenden Netz weitergeleitet.

Unterschieden werden zwei Modi der VPN-Verbindungen:

- Im VPN Roadwarrior-Modus kann das TAINY xMOD-V3 VPN-Verbindungen von Gegenstellen mit unbekannter Adresse annehmen. Das können zum Beispiel Gegenstellen im mobilen Einsatz sein, die ihre IP-Adresse dynamisch beziehen. Das TAINY xMOD-V3 selbst muss über eine feste IP oder über einen DynDNS-Dienst (siehe Kapitel 5.3 und 5.4) erreichbar sein.
  Die VPN-Verbindung muss durch die Gegenstelle aufgebaut werden. Es ist nur eine VPN-Verbindung im Roadwarrior-Modus möglich. VPN-Verbindungen im Standard-Modus können dazu parallel betrieben werden.
- Im VPN Standard-Modus muss die Adresse (IP-Adresse oder Host-Name) des VPN-Gateways der Gegenstelle bekannt sein, damit die VPN-Verbindung aufgebaut werden kann. Die VPN-Verbindung kann wahlweise aufgebaut werden durch das TAINY xMOD-V3 oder durch das VPN-Gateway der Gegenstelle.

Der Aufbau der VPN-Verbindung ist in zwei Phasen aufgeteilt. Zunächst wird in der Phase 1 (ISAKMP = Internet Security Association and Key Management Protocol) die Sicherheitsbeziehung (SA = Security Association) für den Schlüsselaustausch zwischen dem TAINY xMOD-V3 und dem VPN-Gateway der Gegenstelle aufgebaut.

Danach wird dann in der Phase 2 (IPsec = Internet Protocol Security) die Sicherheitsbeziehung (SA = Security Association) für die eigentlichen IPsec-Verbindung zwischen dem TAINY xMOD-V3 und dem VPN-Gateway der Gegenstelle aufgebaut.

Anforderungen an das VPN-Gateway des gegenüberliegenden Netzes

Damit eine IPsec-Verbindung erfolgreich aufgebaut werden kann, muss die VPN-Gegenstelle IPsec mit folgender Konfiguration unterstützen:

- Authentisierung über X.509-Zertifikate, CA-Zertifikate oder Pre-Shared Key (PSK)
- ESP
- Diffie-Hellman Gruppe 1, 2 oder 5
- 3DES oder AES encryption
- MD5 oder SHA-1 Hash Algorithmen
- Tunnel Mode
- Quick Mode
- Main Mode / Agressive Mode
- SA Lifetime (1 Sekunde bis 24 Stunden)

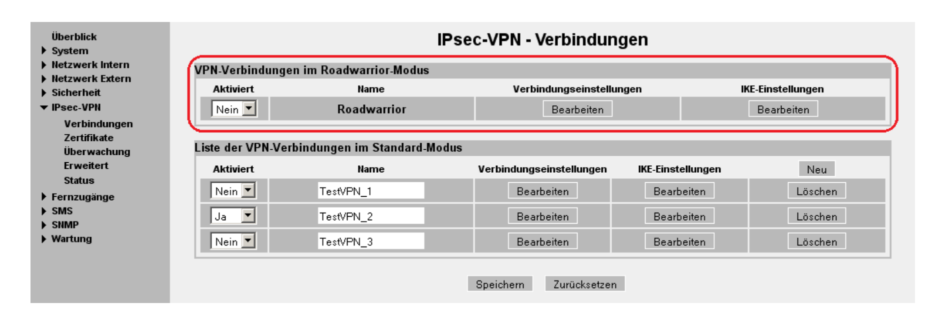
Ist die Gegenstelle ein Rechner unter Windows 2000, muss dazu das Microsoft Windows 2000 High Encryption Pack oder mindestens das Service Pack 2 installiert sein.

Befindet sich die Gegenstelle hinter einem NAT-Router, so muss die Gegenstelle NAT-T unterstützen. Oder aber der NAT-Router muss das IPsec-Protokoll kennen (IPsec/VPN Passthrough).

7.2 IPsec-VPN - Roadwarrior-Modus

IPsec-VPN > Verbindungen

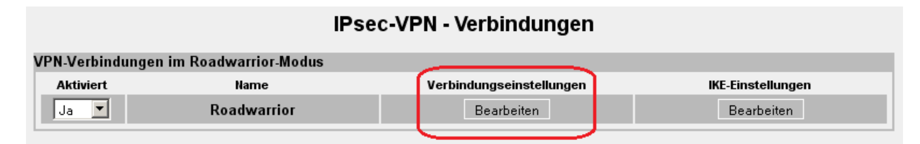
NUR TAINY xMOD-V3

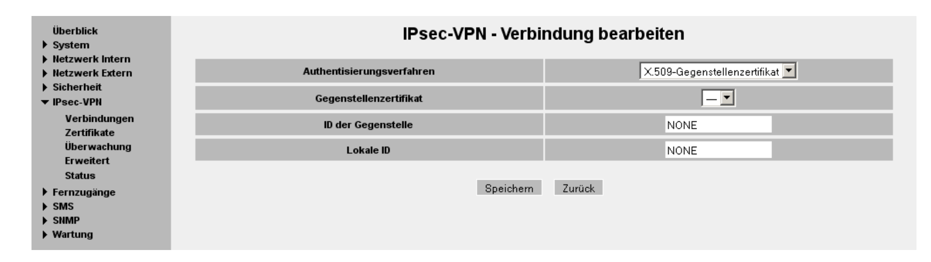


Funktion

Der Roadwarrior-Modus ermöglicht dem TAINY xMOD-V3 die Annahme einer VPN-Verbindung, die von einer Gegenstelle mit unbekannter IP-Adresse eingeleitet wird. Die Gegenstelle muss sich korrekt authentifizieren; auf die Identifikation der Gegenstelle anhand der IP-Adresse oder des Host-Namens der Gegenstelle wird bei dieser VPN-Verbindung aber verzichtet.

Roadwarrior-Modus Verbindung bearbeiten





Funktion

Richten Sie das TAINY xMOD-V3 entsprechend den Absprachen mit dem Systemadministrator der Gegenstelle ein.

Authentisierungs-verfahren

Wählen Sie das Authentisierungsverfahren entsprechend Ihren Vereinbarungen mit dem Administrator der Gegenstelle.

Das TAINY xMOD-V3 unterstützt drei Verfahren:

- X.509-Zertifikat
- CA-Zertifikat
- Pre-Shared Key

X.509-Zertifikat, CA-Zertifikat

Bei den Authentisierungsverfahren X.509-Zertifikat und CA-Zertifikat werden zur Authentifikation Schlüssel verwendet, die zuvor durch eine zertifizierende Stelle (CA = Certification Authority) signiert wurden. Diese Verfahren gelten als besonders sicher. Eine CA kann ein Dienstleister sein, aber z.B. auch der System-Administrator Ihres Projektes, sofern dieser über die notwendigen Software-Werkzeuge verfügt. Die CA erstellt für beide Gegenstellen einer VPN-Verbindung je eine Zertifikatsdatei (PKCS12) mit der Dateiendung *p12. Diese Zertifikatsdatei enthält den öffentlichen und privaten Schlüssel der eigenen Station, das signierte Zertifikat der CA und den öffentlichen Schlüssel der CA. Für das Authentisierungsverfahren X.509 gibt es zusätzlich für jede der beiden Gegenstellen noch eine Schlüsseldatei (*.pem oder *.crt) mit dem öffentlichen Schlüssel der eigenen Station.

X.509-Zertifikat Der Austausch der öffentlichen Schlüssel (Datei mit

Endung *.pem oder *.crt) zwischen dem TAINY xMOD-V3 und dem VPN-Gateway der Gegenstelle erfolgt manuell, zum Beispiel per CD-ROM oder per E-Mail. Zum Laden des Zertifikates gehen Sie vor, wie im Kapitel 7.4 beschrieben.

CA-Zertifikat

Der Austausch der öffentlichen Schlüssel zwischen dem TAINY xMOD-V3 und dem VPN-Gateway der Gegenstelle erfolgt über die Datenverbindung beim Aufbau der VPN-Verbindung. Ein manueller Austausch von Schlüsseldateien entfällt.

Pre-Shared Key (PSK)

Dieses Verfahren wird vor allem durch ältere IPsec-Implementierungen unterstützt. Dabei erfolgt die Authentifikation mit einer zuvor verabredeten Zeichenfolge. Um eine hohe Sicherheit zu erzielen, sollte die Zeichenfolge aus ca. 30 nach dem Zufallsprinzip ausgewählten Klein- und Großbuchstaben sowie Ziffern bestehen.

Folgende Zeichen sind erlaubt:

! $ % & ' ( ) * + , . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ ` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } #

Die Eingabe erfolgt verdeckt.

Gegenstellenzertifikat

Haben Sie als Authentisierungsverfahren *X.509-Gegenstellenzertifikat* gewählt, wird hier die Liste der Zertifikate der Gegenstellen angezeigt, die Sie bereits in das TAINY xMOD-V3 geladen haben. Wählen Sie das Zertifikat für die VPN-Verbindung aus.

ID der Gegenstelle

Lokale ID

Die *Lokale ID* und die *ID der Gegenstelle* werden vom IPsec genutzt, um beim Aufbau der VPN-Verbindung die Gegenstellen eindeutig zu identifizieren. Die eigene *Lokale ID* entspricht dabei der *ID der Gegenstelle* auf Seiten der Gegenstelle und umgekehrt.

Bei Authentisierung mit X.509-Zertifikat oder CA-Zertifikat:

- Belässt man die Werkseinstellung *NONE*, so werden als *Lokale ID* und *ID der Gegenstelle* automatisch die Distinguished Names aus dem eigenen Zertifikat und aus dem von der Gegenstelle übermittelten Zertifikat übernommen.
- Ändert man manuell den Eintrag für die *Lokale ID* oder die *ID der Gegenstelle*, so müssen die korrespondierenden Einträge der Gegenstelle angepasst werden. Die eigene *Lokale ID* muss mit der *ID der Gegenstelle* auf Seiten der Gegenstelle übereinstimmen und umgekehrt. Der manuelle Eintrag für *Lokale ID* oder *ID der Gegenstelle* muss im ASN.1-Format erfolgen,
z.B. "C=XY/O=XY Org/CN=xy.org.org"

Bei Authentisierung mit Pre-Shared Secret Key (PSK):

- Im Roadwarrior-Modus, muss manuell die *ID der Gegenstelle* eingetragen werden. Die *ID der Gegenstelle* muss das Format eines Host-Namens (z.B. RemoteStation.de) oder das Format einer E-Mail-Adresse (remote@station.de) haben und mit der Lokalen ID der Gegenstelle übereinstimmen.
Die *Lokale ID* kann auf *NONE* belassen werden. In diesem Fall wird die IP-Adresse als *Lokale ID* verwendet. Trägt man eine *Lokale ID* ein, muss diese das Format eines Host-Namens (z.B. RemoteStation.de) oder das Format einer E-Mail-Adresse (remote@station.de) haben und auf Seiten der Gegenstelle mit der *ID der Gegenstelle* übereinstimmen.

Roadwarrior-Modus IKE bearbeiten

Funktion

Definieren Sie hier die Eigenschaften der VPN-Verbindung entsprechend Ihren Anforderungen und den Absprachen mit dem Administrator der Gegenstelle.

ISAKMP-SA-Verschlüsselung

IPsec-SA-Verschlüsselung

Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verschlüsselungsverfahren verwendet werden soll für die ISAKMP-SA und die IPsec-SA. Das TAINY xMOD-V3 unterstützt die folgenden Verfahren:

- 3DES-168
- AES-128
- AES-192
- AES-256

AES-128 ist das am häufigsten benutzte Verfahren und ist deshalb als Standard voreingestellt.

Das Verfahren kann für ISAKMP-SA und IPsec-SA unterschiedlich festgelegt werden.

Hinweis

Je mehr Bits ein Verschlüsselungsalgorithmus hat - angegeben durch die angefügte Zahl -, desto sicherer ist er. Das Verfahren AES-256 gilt daher als am sichersten. Allerdings ist der Verschlüsselungsvorgang umso zeitaufwendiger und benötigt mehr Rechenleistung, je länger der Schlüssel ist.

ISAKMP-SA-Hash

IPsec-SA-Hash

Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verfahren zur Berechnung von Prüfsummen/Hash während der ISAKMP-Phase und der IPsec-Phase verwendet werden soll. Zur Auswahl stehen:

- MD5 oder SHA-1 (Automatische Erkennung)
- MD5
- SHA-1

Das Verfahren kann für ISAKMP-SA und IPsec-SA unterschiedlich festgelegt werden.

ISAKMP-SA-Modus

Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verfahren zur Aushandlung der ISAKMP-SA verwendet werden soll. Zur Auswahl stehen:

- Main Mode
- Agressive Mode

Hinweis

Bei Verwendung des Authentisierungsverfahren Pre-Shared Key muss im Roadwarrior-Modus der *Agressive Mode* eingestellt werden.

ISAKMP-SA-Lebensdauer

IPsec-SA Lebensdauer

Die Schlüssel einer IPsec-Verbindung werden in bestimmten Abständen erneuert, um den Aufwand eines Angriffs auf eine IPsec-Verbindung zu erhöhen.

Legen Sie die Lebensdauer der für die ISAKMP-SA und IPsec-SA vereinbarten Schlüssel fest (in Sekunden).

Die Lebensdauer kann für ISAKMP-SA und IPsec-SA unterschiedlich festgelegt werden.

NAT-T

Eventuell befindet sich zwischen dem TAINY xMOD-V3 und den VPN-Gateway des gegenüberliegenden Netzes ein NAT-Router. Nicht alle NAT-Router lassen IPsec-Datenpakete passieren. Daher ist es eventuell erforderlich die IPsec-Datenpakete in UPD-Pakete einzukapseln, so dass sie den NAT-Router passieren können.

An: Wird vom TAINY xMOD-V3 ein NAT-Router erkannt, der die IPsec-Datenpakete nicht passieren lässt, startet automatisch die UDP-Kapselung.

Erzwingen: Bei Aushandlung der Verbindungsparameter der VPN-Verbindung wird darauf bestanden, dass während der Verbindung die Datenpakete gekapselt übertragen werden.

Aus: Die NAT-T-Funktion ist ausgeschaltet

Dead Peer Detection (DPD) aktivieren

Wenn die Gegenstelle das Dead-Peer-Detection-Protokoll (DPD) unterstützt, können die jeweiligen Partner erkennen, ob die IPsec-Verbindung noch gültig ist oder nicht und evtl. neu aufgebaut werden muss. Ohne DPD muss je nach Konfiguration bis zum Ablauf der SA-Lebensdauer gewartet oder die Verbindung manuell neu initiiert werden. Um zu prüfen, ob die IPsec-Verbindung noch gültig ist, sendet die Dead Peer Detection selber DPD-Anfragen zur Gegenstelle. Gibt es keine Antwort, wird die IPsec-Verbindung nach einer Anzahl von erlaubten Fehlversuchen als unterbrochen angesehen.

Warnung

Durch das Versenden der DPD-Anfragen sowie durch die Nutzung von NAT-T steigt die Anzahl der über die Datenfunkdienst-Verbindung (HSPA+, UMTS, EGPRS, GPRS) gesendeten und empfangenen Daten. Abhängig von den gewählten Einstellungen kann das zusätzliche Datenaufkommen 5 MByte im Monat und mehr betragen. Dies kann zu erhöhten Kosten führen.

Ja Die Dead Peer Detection ist eingeschaltet. Das TAINY xMOD-V3 erkennt unabhängig von der Übertragung von Nutzdaten einen Verlust der Verbindung und wartet in diesem Fall auf den Neuaufbau der Verbindung durch die Gegenstellen.

Nein Die Dead Peer Detection ist ausgeschaltet

Verzögerung nach DPD-Anfrage (Sekunden)	Zeitspanne in Sekunden, nach welcher DPD-Anfragen gesendet werden sollen. Diese Anfragen testen, ob die Gegenstelle noch verfügbar ist.
Timeout nach DPD-Anfrage (Sekunden)	Zeitspanne in Sekunden, nach der eine DPD-Anfrage als fehlgeschlagen angesehen wird, wenn auf die DPD-Anfrage keine Antwort erfolgte. Schlägt eine DPD-Anfrage fehl, ist dies zugleich das Intervall mit dem die nächste Anfrage abgesetzt wird, bis die Verbindung endgültig für unterbrochen wird erklärt oder das TAINY xMOD wieder eine DPD-Antwort empfängt.
DPD – Maximale Anzahl an Fehlversuchen	Anzahl der zulässigen Fehlversuche bevor die IPsec-Verbindung als unterbrochen angesehen wird.

Werkseinstellung

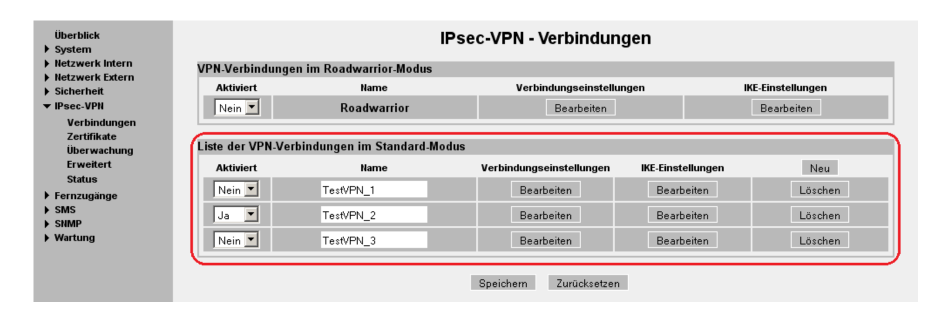
Werkseitig hat das TAINY xMOD-V3 folgende Einstellungen:

Name	**Roadwarrior**
Aktiviert	**Nein (Ausgeschaltet)**
Authentisierungsverfahren	**CA-Zertifikat**
ID der Gegenstelle	**NONE**
Lokale ID	**NONE**
Gegenstellenzertifikat	**-**
Pre Shared Key	**NONE**
ISAKMP-SA-Verschlüsselung	**AES-128**
ISAKMP-SA-Hash (Prüfsumme)	**MD5**
ISAKMP-SA-Modus	**Main Mode**
ISAKMP-SA-Lebensdauer (Sekunden)	**86400**
IPsec-SA-Verschlüsselung	**AES-128**
IPsec-SA-Hash (Prüfsumme)	**MD5**
IPsec-SA-Lebensdauer (Sekunden)	**86400**
NAT-T	**An**
Dead Peer Detection (DPD) aktivieren	**Ja**
Verzögerung nach DPD-Anfrage (Sekunden)	**150**
Timeout nach DPD-Anfrage (Sekunden)	**60**
DPD - Maximale Anzahl an Fehlversuchen	**5**

7.3 IPsec-VPN - Standard-Modus

IPsec-VPN > Verbindungen

NUR TAINY xMOD-V3



Funktion

Angezeigt werden die bereits angelegten VPN-Verbindungen. Sie können jede einzelne Verbindung aktivieren (Aktiviert = *Ja*) oder deaktivieren (Aktiviert = *Nein*). Mit *Neu* können Sie weitere VPN-Verbindungen hinzufügen, mit *Verbindungseinstellungen Bearbeiten* und *IKE-Einstellungen Bearbeiten* können Sie diese einrichten und mit *Löschen* können Sie eine Verbindung entfernen.

Standard-Modus Verbindungen bearbeiten



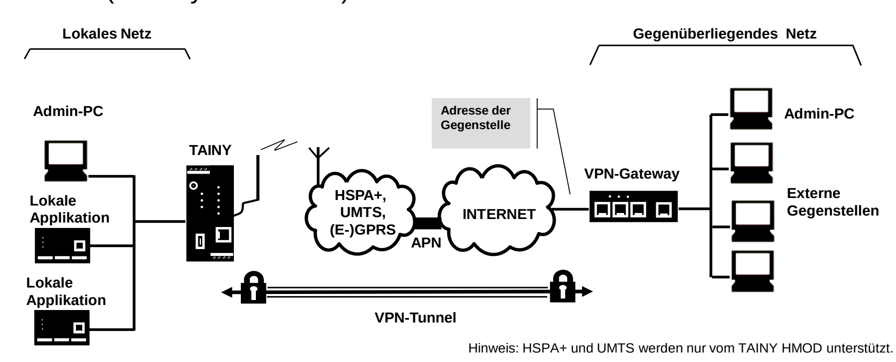


Verbindungsname

Geben Sie der neuen Verbindung hier einen Verbindungsnamen.

Adresse des VPN-Gateways der Gegenstelle

Geben Sie hier die Adresse der Gegenstelle an, entweder als Host-Namen (z.B. myadress.com) oder als IP-Adresse.



Hinweis: HSPA+ und UMTS werden nur vom TAINY HMOD unterstützt.

Authentisierungs-verfahren

Wählen Sie das Authentisierungsverfahren entsprechend Ihren Vereinbarungen mit dem Administrator der Gegenstelle.

Das TAINY xMOD-V3 unterstützt drei Verfahren:

- X.509-Zertifikat
- CA-Zertifikat
- Pre-Shared Key

X.509-Zertifikat, CA-Zertifikat

Bei den Authentisierungsverfahren X.509-Zertifikat und CA-Zertifikat werden zur Authentifikation Schlüssel verwendet, die zuvor durch eine zertifizierende Stelle (CA = Certification Authority) signiert wurden. Diese Verfahren gelten als besonders sicher. Eine CA kann ein Dienstleister sein, aber z.B. auch der System-Administrator Ihres Projektes, sofern dieser über die notwendigen Software-Werkzeuge verfügt. Die CA erstellt für beide Gegenstellen einer VPN-Verbindung je eine Zertifikatsdatei (PKCS12) mit der Dateiendung *p12. Diese Zertifikatsdatei enthält den öffentlichen und privaten Schlüssel der eigenen Station, das signierte Zertifikat der CA und den öffentlichen Schlüssel der CA. Für das Authentisierungsverfahren X.509 gibt es zusätzlich für jede der beiden Gegenstellen noch eine Schlüsseldatei (*.pem oder *.crt) mit dem öffentlichen Schlüssel der eigenen Station.

X.509-Zertifikat	Der Austausch der öffentlichen Schlüssel (Datei mit Endung *.pem oder *.crt) zwischen dem TAINY xMOD-V3 und dem VPN-Gateway der Gegenstelle erfolgt manuell, zum Beispiel per CD-ROM oder per E-Mail. Zum Laden des Zertifikates gehen Sie vor, wie im Kapitel 7.4 beschrieben.
CA-Zertifikat	Der Austausch der öffentlichen Schlüssel zwischen dem TAINY xMOD-V3 und dem VPN-Gateway der Gegenstelle erfolgt über die Datenverbindung beim Aufbau der VPN-Verbindung. Ein manueller Austausch von Schlüsseldateien entfällt.

Pre-Shared Key (PSK)

Dieses Verfahren wird vor allem durch ältere IPsec-Implementierungen unterstützt. Dabei erfolgt die Authentifikation mit einer zuvor verabredeten Zeichenfolge. Um eine hohe Sicherheit zu erzielen, sollte die Zeichenfolge aus ca. 30 nach dem Zufallsprinzip ausgewählten Klein- und Großbuchstaben sowie Ziffern bestehen.

Folgende Zeichen sind erlaubt:

! $ % & ' ( ) * + , . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ ` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } #

Die Eingabe erfolgt verdeckt.

Gegenstellenzertifikat

Haben Sie als Authentisierungsverfahren *X.509-Gegenstellenzertifikat* gewählt, wird hier die Liste der Zertifikate der Gegenstellen angezeigt, die Sie bereits in das TAINY xMOD-V3 geladen haben. Wählen Sie das Zertifikat für die VPN-Verbindung aus.

ID der Gegenstelle

Lokale ID

Die *Lokale ID* und die *ID der Gegenstelle* werden vom IPsec genutzt, um beim Aufbau der VPN-Verbindung die Gegenstellen eindeutig zu identifizieren.

Bei Authentisierung mit X.509-Zertifikat oder CA-Zertifikat:

- Belässt man die Werkseinstellung *NONE*, so werden als *Lokale ID* und *ID der Gegenstelle* automatisch die Distinguished Names aus dem eigenen Zertifikat und aus dem von der Gegenstelle übermittelten Zertifikat übernommen und verwendet.
- Ändert man manuell den Eintrag für die *Lokale ID* oder die *ID der Gegenstelle*, so müssen die korrespondierenden Einträge der Gegenstelle angepasst werden. Die eigene *Lokale ID* muss mit der *ID der Gegenstelle* auf Seiten der Gegenstelle übereinstimmen und umgekehrt. Der manuelle Eintrag für *Lokale ID* oder *ID der Gegenstelle* muss im ASN.1-Format erfolgen, z.B. "C=XY/O=XY Org/CN=xy.org.org"

Bei Authentisierung mit Pre-Shared Key (PSK):

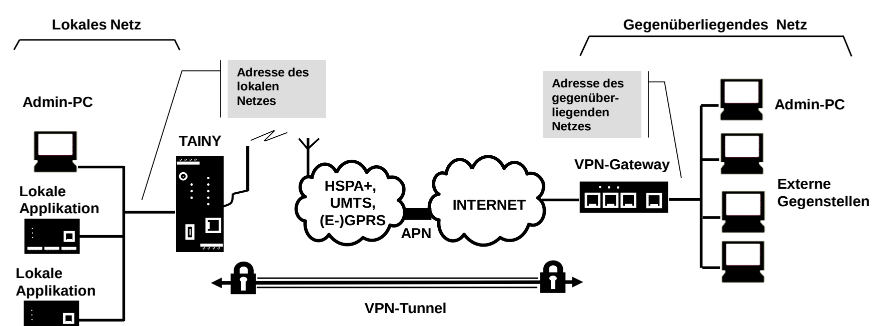
- Belässt man die Werkseinstellung *NONE*, so werden automatisch als *Lokale ID* die eigene IP-Adresse und als *ID der Gegenstelle* die IP-Adresse der Gegenstelle übernommen.
- Ändert man manuell den Eintrag für die *Lokale ID* oder für die *ID der Gegenstelle*, so müssen die Einträge das Format eines Host-Namens (z.B. RemoteStation.de) oder das Format einer E-Mail-Adresse (remote@station.de) haben. Die eigene Lokale ID muss mit der *ID der Gegenstelle* auf Seiten der Gegenstelle übereinstimmen und umgekehrt.

Hinweis

Wenn bei Pre-Shared Key (PSK) nicht die IP-Adresse als *ID der Gegenstelle* verwendet wird, muss als ISAKMP-SA-Modus der *Agressive mode* eingestellt werden.

IP-Adresse des gegenüberliegenden Netzes

Tragen Sie hier die IP-Adresse (z.B. 123.123.123.123) des gegenüberliegenden Netzes ein. Das gegenüberliegende Netz kann auch nur ein einzelner Rechner sein.



Netzmaske des gegenüberliegenden Netzes

Tragen Sie hier die Netzwerkmaske (z.B. 255.255.255.0) des gegenüberliegenden Netzes ein. Das gegenüberliegende Netz kann auch nur ein einzelner Rechner sein.

1-zu-1-NAT für das gegenüberliegende Netz aktivieren

Das TAINY xMOD-V3 verfügt über eine 1-zu-1-NAT-Funktion zum gegenüberliegenden Netz.

Der Adressbereich des gegenüberliegenden Netzes auf der VPN-Verbindung wird im TAINY xMOD-V3 festgelegt über die

- *IP-Adresse des gegenüberliegenden Netzes* und die
- *Netzmaske des gegenüberliegenden Netzes* (s.o.)

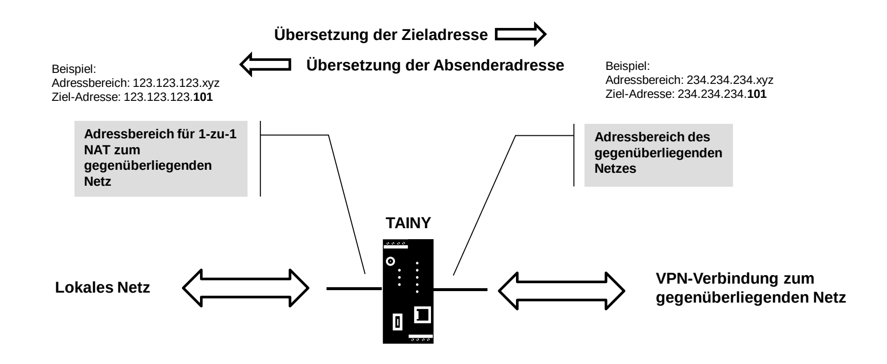
Ist 1-zu-1-NAT abgeschaltet, müssen lokale Applikationen diesen Adressbereich zur Adressierung von Gegenstellen im gegenüberliegenden Netz verwenden.

Ist 1-zu-1-NAT aktiviert, kann ein lokal verwendeter Adressbereich definiert werden, über den lokale Applikationen Gegenstellen im gegenüberliegenden Netz adressieren können.

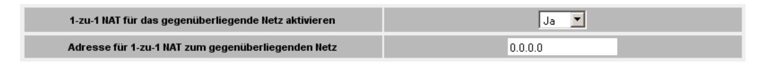
Die 1-zu-1-NAT-Funktion im TAINY xMOD-V3 bildet dann den lokal definierten Adressbereich des gegenüberliegenden Netzes auf den tatsächlichen Adressbereich des gegenüberliegenden Netzes auf der VPN-Verbindung ab.

Der lokal verwendete Adressbereich des gegenüberliegenden Netzes wird festgelegt über die

- *Adresse für 1-zu-1-NAT zum gegenüberliegenden Netz* und die
- *Netzmaske des gegenüberliegenden Netzes*



Ja Das TAINY xMOD-V3 verwendet 1-zu-1-NAT zum gegenüberliegenden Netz.



1-zu-1 NAT für das gegenüberliegende Netz aktivieren	Ja
Adresse für 1-zu-1 NAT zum gegenüberliegenden Netz	0.0.0.0

Geben Sie als *Adresse für 1-zu-1-NAT zum gegenüberliegenden Netz* die lokal verwendete Zieladresse ein.

Nein Das TAINY xMOD-V3 verwendet kein 1-zu-1-NAT zum gegenüberliegenden Netz.

Adresse des lokalen Netzes

Tragen Sie hier die IP-Adresse (z.B. 123.123.123.123) des lokalen Netzes ein. Das lokale Netz kann auch nur ein einzelner Rechner sein.

Netzmaske des lokalen Netzes

Tragen Sie hier die Netzwerkmaske (z.B. 255.255.255.0) des lokalen Netzes ein. Das lokale Netz kann auch nur ein einzelner Rechner sein.

1-zu-1-NAT für das lokale Netz aktivieren

Der Adressbereich des lokalen Netzes auf der VPN-Verbindung wird im TAINY xMOD-V3 festgelegt über die

- *Adresse des lokalen Netzes* und die
- *Netzmaske des lokalen Netzes* (s.o.)

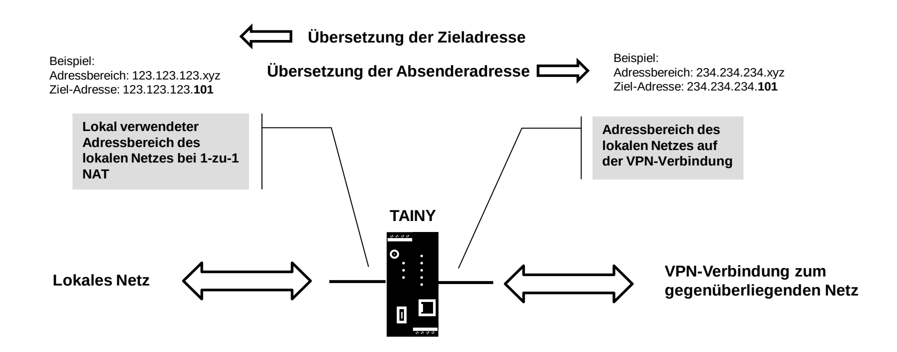
Ist 1-zu-1-NAT abgeschaltet, müssen die Adressen lokaler Applikationen in diesem Adressbereich liegen, um über die VPN-Verbindung von Gegenstellen im gegenüberliegenden Netz adressiert werden zu können.

Ist 1-zu-1-NAT aktiviert, kann ein lokal verwendeter Adressbereich für das lokale Netz definiert werden, der sich von dem Adressbereich, der auf der VPN-Verbindung genutzt wird unterscheidet.

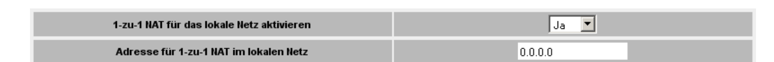
Die 1-zu-1-NAT-Funktion im TAINY xMOD-V3 bildet dann den lokalen Adressbereich des lokalen Netzes auf den Adressbereich des lokalen Netzen auf der VPN-Verbindung ab.

Der lokal verwendete Adressbereich des lokalen Netzes wird festgelegt über die

- *Adresse für 1-zu-1-NAT im lokalen Netz* und die
- *Netzmaske des lokalen Netzes*



Ja Das TAINY xMOD-V3 verwendet 1-zu-1-NAT zum lokalen Netz.



1-zu-1 NAT für das lokale Netz aktivieren	Ja
Adresse für 1-zu-1 NAT im lokalen Netz	0.0.0.0

Geben Sie als *Adresse für 1-zu-1-NAT im lokalen Netz* die lokal verwendete Zieladresse ein.

Nein Das TAINY xMOD-V3 verwendet kein 1-zu-1-NAT zum lokalen Netz.

Auf Verbindungs-aufbau durch die Gegenstelle warten

Ja Das TAINY xMOD-V3 wartet darauf, dass das VPN-Gateway des gegenüberliegenden Netzes den Aufbau der VPN-Verbindung einleitet.

Nein Das TAINY xMOD-V3 leitet den Verbindungsaufbau ein.

Firewall-Regeln für VPN-Tunnel

Siehe Kapitel 7.5

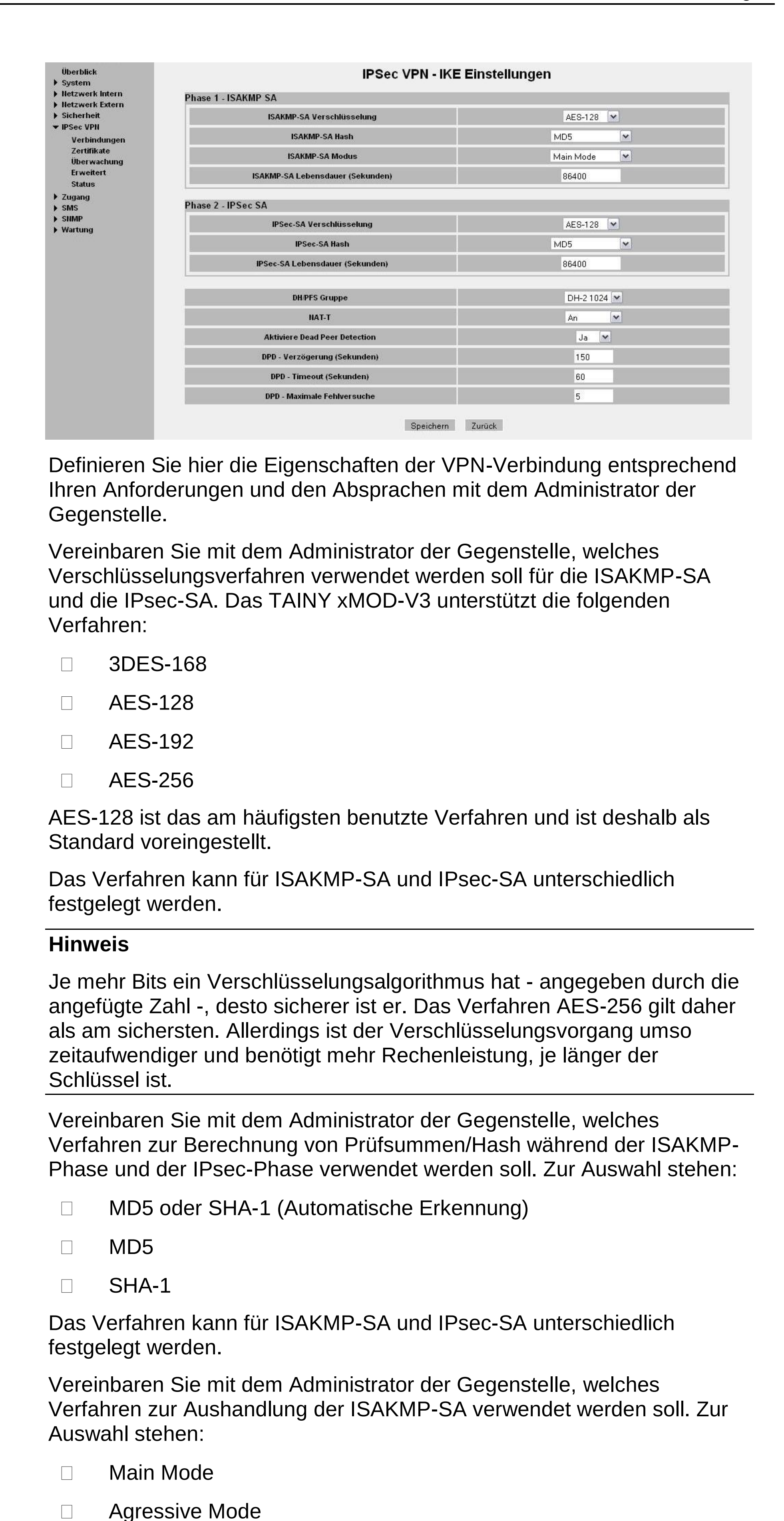
Standard-Modus

IKE bearbeiten



Liste der VPN-Verbindungen im Standard-Modus

Aktiviert	Name	Verbindungseinstellungen	IKE-Einstellungen	Neu
Nein	TestVPN_1	Bearbeiten	Bearbeiten	Löschen



Funktion

Definieren Sie hier die Eigenschaften der VPN-Verbindung entsprechend Ihren Anforderungen und den Absprachen mit dem Administrator der Gegenstelle.

ISAKMP-SA-Verschlüsselung

IPsec-SA-Verschlüsselung

Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verschlüsselungsverfahren verwendet werden soll für die ISAKMP-SA und die IPsec-SA. Das TAINY xMOD-V3 unterstützt die folgenden Verfahren:

- 3DES-168
- AES-128
- AES-192
- AES-256

AES-128 ist das am häufigsten benutzte Verfahren und ist deshalb als Standard voreingestellt.

Das Verfahren kann für ISAKMP-SA und IPsec-SA unterschiedlich festgelegt werden.

Hinweis

Je mehr Bits ein Verschlüsselungsalgorithmus hat - angegeben durch die angefügte Zahl -, desto sicherer ist er. Das Verfahren AES-256 gilt daher als am sichersten. Allerdings ist der Verschlüsselungsvorgang umso zeitaufwendiger und benötigt mehr Rechenleistung, je länger der Schlüssel ist.

ISAKMP-SA-Hash

IPsec-SA-Hash

Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verfahren zur Berechnung von Prüfsummen/Hash während der ISAKMP-Phase und der IPsec-Phase verwendet werden soll. Zur Auswahl stehen:

- MD5 oder SHA-1 (Automatische Erkennung)
- MD5
- SHA-1

Das Verfahren kann für ISAKMP-SA und IPsec-SA unterschiedlich festgelegt werden.

ISAKMP-SA-Modus

Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verfahren zur Aushandlung der ISAKMP-SA verwendet werden soll. Zur Auswahl stehen:

- Main Mode
- Agressive Mode

ISAKMP-SA-Lebensdauer IPsec-SA-Lebensdauer	Die Schlüssel einer IPsec-Verbindung werden in bestimmten Abständen erneuert, um den Aufwand eines Angriffs auf eine IPsec-Verbindung zu erhöhen. Legen Sie die Lebensdauer der für die ISAKMP-SA und IPsec-SA vereinbarten Schlüssel fest (in Sekunden). Die Lebensdauer kann für ISAKMP-SA und IPsec-SA unterschiedlich festgelegt werden.
DH/PFS-Gruppe	Vereinbaren Sie mit dem Administrator der Gegenstelle die DH-Gruppe für den Schlüsselaustausch.
NAT-T	Eventuell befindet sich zwischen dem TAINY xMOD-V3 und den VPN-Gateway des gegenüberliegenden Netzes ein NAT-Router. Nicht alle NAT-Router lassen IPsec-Datenpakete passieren. Daher ist es eventuell erforderlich die IPsec-Datenpakete in UPD-Pakete einzukapseln, um den NAT-Router passieren zu können. *An:* Wird vom TAINY xMOD-V3 ein NAT-Router erkannt, der die IPsec-Datenpakete nicht passieren lässt, startet automatisch die UDP-Kapselung. *Erzwingen:* Bei Aushandlung der Verbindungsparameter der VPN-Verbindung wird darauf bestanden, dass während der Verbindung die Datenpakete gekapselt übertragen werden. *Aus:* Die NAT-T-Funktion ist ausgeschaltet
Aktiviere Dead Peer Detection	Wenn die Gegenstelle das Dead-Peer-Detection-Protokoll (DPD) unterstützt, können die jeweiligen Partner erkennen, ob die IPsec-Verbindung noch gültig ist oder nicht und evtl. neu aufgebaut werden muss. Ohne DPD muss je nach Konfiguration bis zum Ablauf der SA-Lebensdauer gewartet oder die Verbindung manuell neu initiiert werden. Um zu prüfen, ob die IPsec-Verbindung noch gültig ist, sendet die Dead Peer Detection selber DPD-Anfragen zur Gegenstelle. Gibt es keine Antwort, wird die IPsec-Verbindung nach einer Anzahl von erlaubten Fehlversuchen als unterbrochen angesehen. **Warnung** Durch das Versenden der DPD-Anfragen sowie durch die Nutzung von NAT-T steigt die Anzahl der über die Datenfunkdienst-Verbindung (HSPA+, UMTS, EGPRS, GPRS) gesendeten und empfangenen Daten. Abhängig von den gewählten Einstellungen kann das zusätzliche Datenaufkommen 5 MByte im Monat und mehr betragen. Dies kann zu erhöhten Kosten führen. *Ja* Die Dead Peer Detection ist eingeschaltet. Es wird versucht, die IPsec-Verbindung neu aufzubauen, wenn diese für tot erklärt wurde, unabhängig von der Übertragung von Nutzdaten. *Nein* Die Dead Peer Detection ausgeschaltet
Verzögerung nach DPD-Anfrage (Sekunden)	Zeitspanne in Sekunden, nach welcher DPD-Anfragen gesendet werden sollen. Diese Anfragen testen, ob die Gegenstelle noch verfügbar ist.
Timeout nach DPD-Anfrage (Sekunden)	Zeitspanne in Sekunden, nach der eine DPD-Anfrage als fehlgeschlagen angesehen wird, wenn auf die DPD-Anfrage keine Antwort erfolgt. Schlägt eine DPD-Anfrage fehl, ist dies zugleich das Intervall mit dem die nächste Anfrage abgesetzt wird, bis die Verbindung endgültig für unterbrochen wird erklärt oder das TAINY xMOD wieder eine DPD-Antwort empfängt.
DPD – Maximale Anzahl an	Anzahl der zulässigen Fehlversuche bevor die IPsec-Verbindung als unterbrochen angesehen wird.

Fehlversuchen

Werkseinstellung

Werkseitig verwendet das TAINY xMOD-V3 folgende Einstellungen für eine neu angelegte Verbindung:

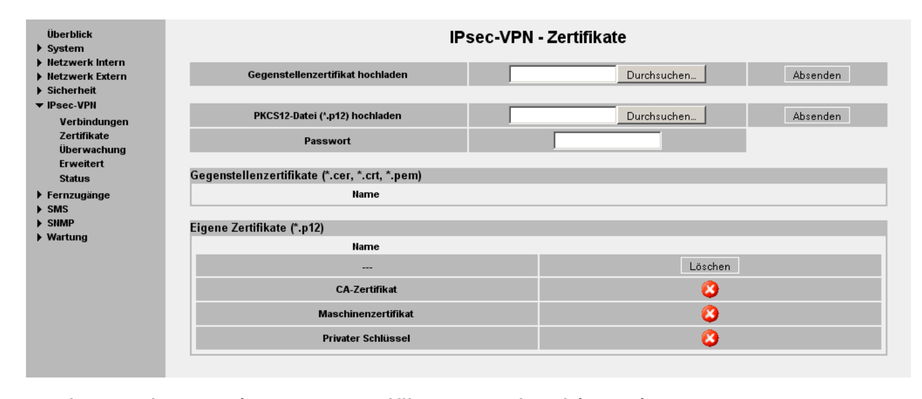
Name	**NewConnection**
Aktiviert	**Nein (Ausgeschaltet)**
Adresse des VPN-Gateways der Gegenstelle	**NONE**
Authentisierungsverfahren	**CA-Zertifikat**
Gegenstellenzertifikat	**-**
Pre Shared Key	**NONE**
ID der Gegenstelle	**NONE**
Lokale ID	**NONE**
IP-Adresse des gegenüberliegenden Netzes	**192.168.2.1**
Netzmaske des gegenüberliegenden Netzes	**255.255.255.0**
1-zu-1 NAT für das gegenüberliegende Netz aktivieren	**Nein**
Adresse für 1-zu-1 NAT zum gegenüberliegenden Netz	**0.0.0.0**
Adresse des lokalen Netzes	**192.168.1.1**
Netzmaske des lokalen Netzes	**255.255.255.0**
1-zu-1 NAT für das lokale Netz aktivieren	**Nein**
Adresse für 1-zu-1 NAT im lokalen Netz	**0.0.0.0**
Auf Verbindungsaufbau durch die Gegenstelle warten	**Nein**
ISAKMP-SA-Verschlüsselung	**AES-128**
ISAKMP-SA-Hash (Prüfsumme)	**MD5**
ISAKMP-SA-Modus	**Main Mode**
ISAKMP-SA-Lebensdauer (Sekunden)	**86400**
IPsec-SA-Verschlüsselung	**AES-128**
IPsec-SA-Hash (Prüfsumme)	**MD5**
IPsec-SA-Lebensdauer (Sekunden)	**86400**
DH/PFS-Gruppe	**DH-2 1024**
NAT-T	**An**
Dead-Peer-Detection (DPD) aktivieren	**Ja**
Verzögerung nach DPD-Anfrage (Sekunden)	**150**
Timeout nach DPD-Anfrage (Sekunden)	**60**
DPD – Maximale Anzahl an	**5**

Fehlversuchen

7.4 IPsec-VPN - Zertifikate laden

IPsec-VPN - Zertifikate

NUR TAINY xMOD-V3



Funktion

Laden und Verwalten von Zertifikaten und Schlüsseln.

Gegenstellenzertifikat hochladen

Laden Sie hier Schlüsseldateien (*.pem, *.crt) mit Gegenstellenzertifikaten und öffentlichen Schlüsseln von Gegenstellen in das TAINY xMOD-V3. Die Dateien müssen dazu auf dem Admin-PC gespeichert sein. Ein Gegenstellen-Zertifikat wird nur beim Authentisierungsverfahren mit X.509-Zertifikat benötigt.

PKCS12-Datei (*.p12) hochladen

Laden Sie hier die Zertifikatsdatei (PKCS12-Datei) mit der Dateiendung .p12 in das TAINY xMOD-V3. Die Zertifikatsdatei muss dazu auf dem Admin-PC gespeichert sein.

Achtung

Befindet sich bereits eine Zertifikatsdatei im Gerät, muss diese vor dem Laden einer neuen Datei gelöscht werden.

Passwort

Die Zertifikatsdatei (PKCS12-Datei) ist mit einem Passwort geschützt. Geben Sie hier das Passwort ein, das Sie mit der Zertifikatsdatei erhalten haben.

Gegenstellenzertifikate (*.cer, *.crt, *.pem)

An dieser Stelle werden alle geladenen Gegenstellenzertifikate in einer Liste angezeigt. Mit *Löschen* können Sie Gegenstellenzertifikate, die nicht mehr benötigt werden, wieder entfernen.

Eigene Zertifikate (*.p12)

An dieser Stelle wird der Name und Zustand der geladenen Zertifikatsdatei (PKCS12-Datei) angezeigt.


Der jeweilige Bestandteil der Zertifikatsdatei ist vorhanden

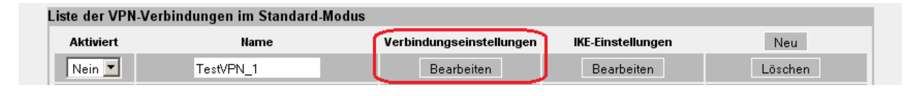

Der jeweilige Bestandteil fehlt oder das eingegebene Passwort ist falsch

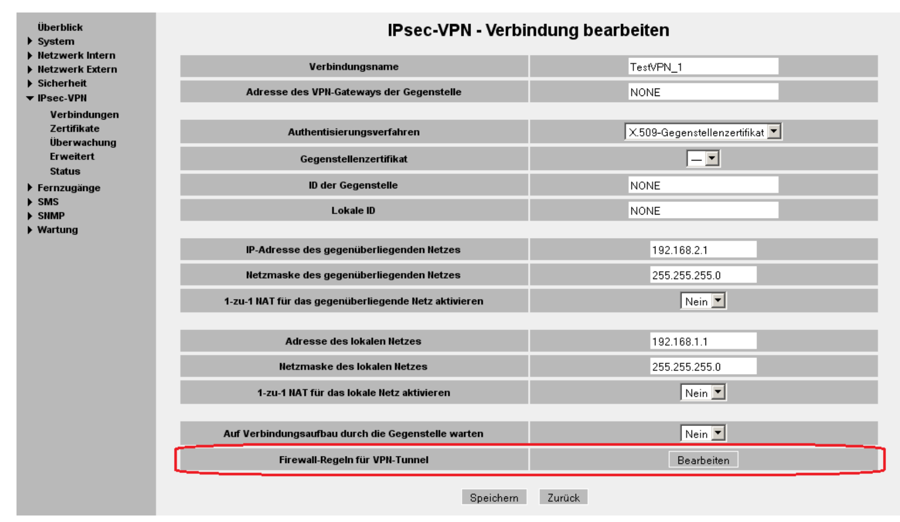
7.5 Firewall-Regeln für VPN-Tunnel

Firewall-Regeln für VPN-Tunnel

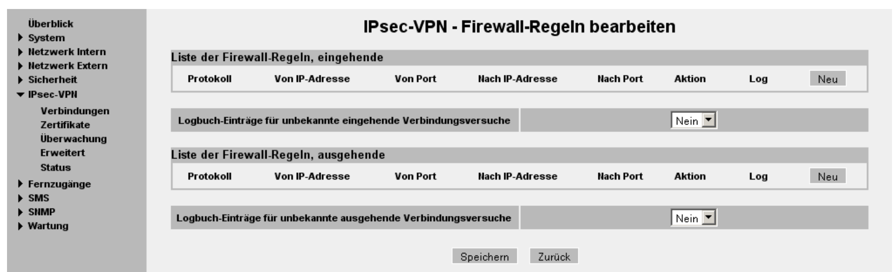
NUR TAINY xMOD-V3

Die Oberfläche zum Einrichten der Firewall-Regeln für VPN-Tunnel finden Sie unter IPsec-VPN > Verbindungen:





IPsec-VPN –Firewall-Regeln bearbeiten



Funktion

Die IPsec-VPN-Verbindung wird grundsätzlich als sicher angesehen. So ist der Datenverkehr über diese Verbindung standardmäßig nicht beschränkt. Es ist aber möglich Firewall-Regeln für die VPN-Verbindung zu erstellen

Gehen Sie bei der Einrichtung der Firewall-Regeln für die VPN-Verbindung vor, wie bei der Einrichtung der Paketfilter-Funktion der allgemeinen Firewall (siehe Kapitel 6.1). Die hier festgelegten Regeln, gelten aber nur für die jeweilige VPN-Verbindung.

Werkseinstellung

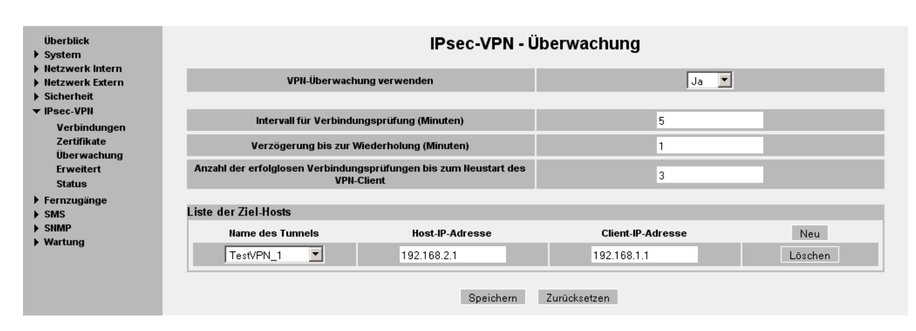
Werkseitig verwendet das TAINY xMOD-V3 folgende Einstellungen für eine neu angelegte Verbindung (eingehend und ausgehend):

Protokoll	**Alle**
Von IP-Adresse	**0.0.0.0/0**
Von Port	**ANY**
Nach IP-Adresse	**0.0.0.0/0**
Nach Port	**ANY**
Aktion	**Verwerfen**
Log	**Nein (Ausgeschaltet)**
Logbuch-Einträge für unbekannte eingehende Verbindungsversuche	**Nein (Ausgeschaltet)**
Logbuch-Einträge für unbekannte ausgehende Verbindungsversuche	**Nein (Ausgeschaltet)**

7.6 Überwachung der VPN-Verbindungen

IPsec-VPN > Überwachung

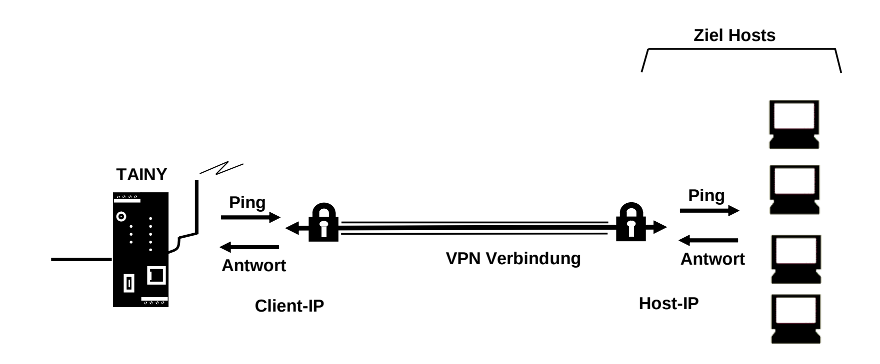
NUR TAINY xMOD-V3



Funktion

Mit der Überwachung der VPN-Verbindungen überprüft das TAINY xMOD-V3 aufgebaute VPN-Verbindungen. Dazu sendet das TAINY xMOD-V3 über die VPN-Verbindung in regelmäßigen Zeitabständen Ping-Pakete (ICMP) an eine oder mehrere Gegenstellen (Ziel Hosts). Dies geschieht unabhängig von den Nutzdaten. Für jede VPN-Verbindung kann eine eigene Überwachung eingerichtet werden.

Erhält das TAINY xMOD-V3 von mindestens einer der adressierten Gegenstellen eine Antwort auf einen Ping, ist die VPN-Verbindung noch funktionsbereit.



Antwortet keine der Gegenstellen auf den Ping, findet folgender Ablauf statt:

- festgelegte Anzahl an Wiederholungen des Ping-Tests
- festgelegte Anzahl an Wiederholungen des Ping-Tests, jeweils mit Neuaufbau des/der getesteten Tunnel
- Neustart des VPN Client

Voraussetzung für diesen Ablauf ist, dass der Tunnel aufgebaut werden kann, aber die zum Test verwendete Gegenstelle nicht erreicht wird. Sobald ein Ping-Test erfolgreich durchgeführt wurde, wird dieser Ablauf unterbrochen. Kann der Tunnel generell nicht aufgebaut werden, greift der in Kapitel 7.7 beschriebene Ablauf für das Fehlschlagen beim Aufbau von Tunnelverbindungen.

Warnung

Durch das Versenden der Ping-Pakete (ICMP) steigt die Anzahl der über die Datenfunkdienst-Verbindung (HSPA+, UMTS, EGPRS oder GPRS) gesendeten und empfangenen Daten. Abhängig von den gewählten Einstellungen kann das zusätzliche Datenaufkommen 4,5 MByte im Monat und mehr betragen. Dies kann zu erhöhten Kosten führen.

Hinweis

Die Überwachung der VPN-Verbindungen mittels Ping überschneidet sich zum Teil mit den Überwachungsfunktionen der Dead Peer Detection. Bei aktivierter Ping-Überwachung kann die DPD – Verzögerung erhöht werden.

VPN-Überwachung verwenden	*Ja*	VPN-Überwachung eingeschaltet
	Nein	VPN-Überwachung ausgeschaltet

Intervall für Verbindungsprüfung (Minuten)

An dieser Stelle wird festgelegt, in welchen Zeitintervallen die Ping-Pakete über die überwachten VPN-Verbindungen (VPN-Tunnel) gesendet werden.

Die Angabe erfolgt in Minuten.

Verzögerung bis zur Wiederholung (Minuten)

An dieser Stelle wird die Wartezeit festgelegt, nach deren Ablauf nach einer erfolglosen Ping-Prüfung (keine Antwort auf den Ping), der Ping wiederholt wird.

Die Angabe erfolgt in Minuten.

Anzahl der erfolglosen Verbindungsprüfungen bis zum Neustart des VPN-Client

Dieser Parameter legt die Anzahl der Ping-Test-Wiederholungen an zwei Stellen des Ablaufs fest:

- Anzahl der Wiederholungen des Ping-Tests bis zum ersten Neustart der VPN-Verbindung
- Anzahl der Ping-Tests mit jeweiligem Neustart der Tunnelverbindung bzw. Tunnelverbindungen bis zum Neustart des VPN-Client

Liste der Ziel-Hosts	*Name des Tunnels*	Legen Sie hier fest, welche VPN-Verbindungen (VPN-Tunnel) überwacht werden sollen. Richten Sie mit *Neu* für eine der bereits angelegten VPN-Verbindungen eine Überwachung ein oder beenden Sie mit *Löschen* die Überwachung einer VPN-Verbindung.
	Host-IP-Adresse	Wählen Sie hierüber die IP-Adresse der Gegenstelle (Ziel-Host) aus.
	Client-IP-Adresse	Geben Sie hier als Absender IP eine beliebige ungenutzte IP-Adresse aus dem lokalen Netzbereich der jeweiligen VPN-Verbindung an.

Werkseinstellung

Werkseitig verwendet das TAINY xMOD-V3 folgende Einstellungen:

VPN-Überwachung verwenden	**Nein**
Intervall für Verbindungsprüfung (Minuten)	**5**
Verzögerung bis zur Wiederholung (Minuten)	**1**
Anzahl der erfolglosen Verbindungsprüfungen bis zum Neustart des VPN-Client	**3**
Name des Tunnels	**-**
Host-IP-Adresse	**192.168.2.1**
Client-IP-Adresse	**192.168.1.1**

7.7 Erweiterte Einstellungen bei VPN-Verbindungen

IPsec-VPN > Erweitert

NUR TAINY xMOD-V3

Überblick
System
Netzwerk Intern
Netzwerk Extern
Sicherheit
IPsec-VPN
Verbindungen
Zertifikate
Überwachung
Erweitert
Status
Fernzugänge
SMS
SNMP
Wartung

IPsec-VPN - Erweitert

Keepalive-Intervall für NAT-T (Sekunden)	60
Phase-1-Timeout (Sekunden)	15
Phase-2-Timeout (Sekunden)	10
Maximale Anzahl der Verbindungsaufbauversuche bis zum Neustart des VPN-Client	5
Maximale Anzahl der Verbindungsaufbauversuche nach Neustart des VPN-Client bis zum Neustart des Geräts	2
DynDNS-Tracking	Ja
Intervall für DynDNS-Tracking (Minuten)	5
Neustart des VPN-Client bei DPD	Nein

Speichern Zurücksetzen

Funktion	Einstellen spezieller Wartezeiten und Intervalle bei VPN-Verbindungen.
Keepalive-Intervall für NAT-T (Sekunden)	Ist NAT-T aktiviert (vgl. Kapitel 7.3) dann werden periodisch Keepalive-Datenpakete vom TAINY xMOD-V3 durch die VPN-Verbindung gesendet. Dies soll verhindern, dass ein NAT-Router zwischen TAINY xMOD-V3 und der Gegenstelle in Ruhephasen ohne Datenverkehr, die Verbindung unterbricht. Das Intervall zwischen den Keepalive-Datenpaketen können Sie hier ändern.
Phase-1-Timeout (Sekunden)	Das Phase 1 Timeout bestimmt, wie lange das TAINY xMOD-V3 abwartet, bis ein Authentisierungsverfahren der ISAKMP-SA abgeschlossen ist. Wird das eingestellte Timeout überschritten, wird das Authentisierungsverfahren abgebrochen und neu gestartet. Das Timeout können Sie hier ändern.
Phase-2-Timeout (Sekunden)	Das Phase 2 Timeout bestimmt, wie lange das TAINY xMOD-V3 abwartet, bis ein Authentisierungsverfahren der IPsec-SA abgeschlossen ist. Wird das eingestellte Timeout überschritten, wird das Authentisierungsverfahren abgebrochen und neu gestartet. Das Timeout können Sie hier ändern.
Maximale Anzahl der Verbindungsaufbau-versuche bis zum Neustart des VPN-Client	Schlägt ein VPN-Verbindungsaufbau fehl, wird der Verbindungsaufbau vom TAINY xMOD-V3 wiederholt. Geben Sie hier die Anzahl der erfolglosen Versuche ein, bevor das TAINY xMOD-V3 seinen VPN-Client neu startet um dann erneut den Verbindungsaufbau einzuleiten.
Maximale Anzahl der Verbindungsaufbau-versuche nach Neustart des VPN-Client bis zum Neustart des Geräts	Schlägt nach dem Neustart des VPN-Clients der VPN-Verbindungsaufbau fehl, wird der Verbindungsaufbau vom TAINY xMOD-V3 wiederholt. Geben Sie hier die Anzahl der erfolglosen Versuche ein, bevor das TAINY xMOD-V3 einen Reboot durchführt, um dann erneut den VPN-Verbindungsaufbau einzuleiten.
DynDNS-Tracking	Bezieht das VPN-Gateway der Gegenstelle die IP-Adresse von einem DynDNS-Dienst und wird keine Dead Peer Detection verwendet, ist es sinnvoll, dass das TAINY xMOD-V3 regelmäßig überprüft, ob das VPN-Gateway der Gegenstelle noch erreichbar ist. Das DynDNS Tracking übernimmt diese Funktion. Mit Ja, wird die Funktion aktiviert, mit Nein deaktiviert.
Intervall für DynDNS-Tracking (Minuten)	Stellen Sie hier ein, in welchen Abständen per DynDNS Tracking geprüft werden soll, ob die Gegenstelle noch erreichbar ist.
Neustart des VPN-Client bei DPD	Stellen Sie hier ein, ob der VPN-Client bei Zuschlagen der Dead Peer Detection (DPD) neu gestartet werden soll.

Werkseinstellung

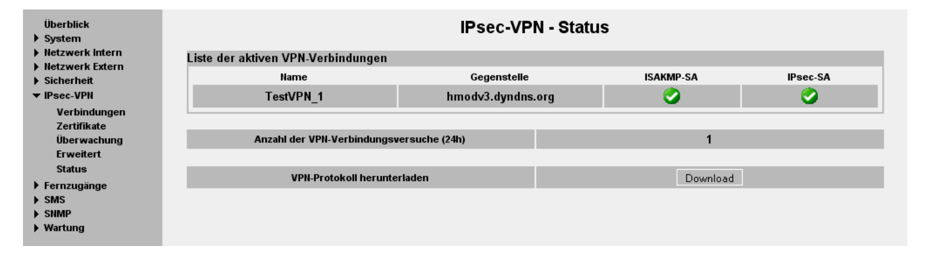
Werkseitig verwendet das TAINY xMOD-V3 folgende Einstellungen:

Einstellung	Wert
Keepalive-Intervall für NAT-T (Sekunden)	**60**
Phase-1-Timeout (Sekunden)	**15**
Phase-2-Timeout (Sekunden)	**10**
Maximale Anzahl der Verbindungsaufbauversuche bis zum Neustart des VPN-Client	**5**
Maximale Anzahl der Verbindungsaufbauversuche nach Neustart des VPN-Client bis zum Neustart des Geräts	**2**
DynDNS-Tracking	**Nein**
Intervall für DynDNS- Tracking (Minuten)	**5**
Neustart des VPN-Client bei DPD	**Nein**

7.8 Status der VPN-Verbindungen

IPsec-VPN > Status

NUR TAINY xMOD-V3



Funktion

Anzeige des Status der aktivierten VPN-Verbindungen und Möglichkeit eine Protokolldatei auf den Admin-PC zu laden.

Liste der aktiven VPN-Verbindungen

Die jeweilige Sicherheitsbeziehung (SA = Security Association) ist erfolgreich aufgebaut.



Die Sicherheitsbeziehung besteht nicht.

Anzahl der VPN-Verbindungsversuche (24h)

Zeigt die Anzahl der Versuche seit 0:00 Uhr (Systemzeit) an, die aktivierten VPN-Verbindungen aufzubauen.

VPN-Protokoll herunterladen

Mit dieser Funktion können Sie die VPN-Protokolldatei auf den Admin-PC herunterladen.

8 OpenVPN-Verbindung

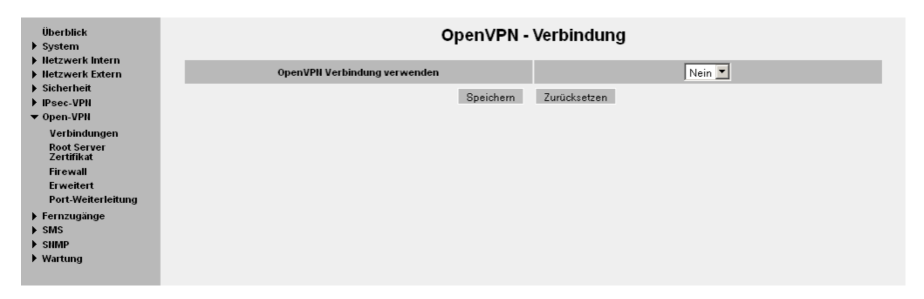
NUR TAINY xMOD-V3

Hinweis zum Funktionsumfang

Der Menüpunkt OpenVPN findet sich nur bei TAINY xMOD-V3-Geräten. Nur TAINY xMOD-V3-Geräte unterstützen OpenVPN-Verbindungen.

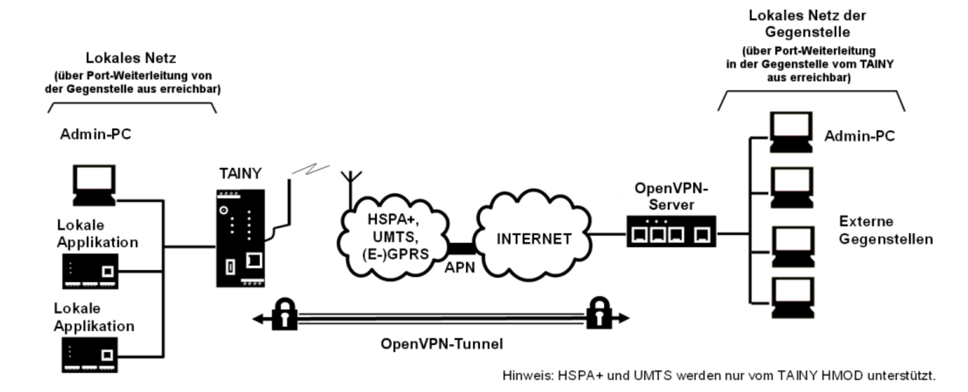
8.1 Einleitung

NUR TAINY xMOD-V3



Funktion

Das TAINY xMOD-V3 kann sich per OpenVPN mit einem entfernten OpenVPN-Server verbinden. Die IP-Datenpakete, die zwischen den beiden OpenVPN-Endpunkten ausgetauscht werden, sind verschlüsselt und durch den OpenVPN-Tunnel gegen unerlaubte Manipulationen geschützt. So können auch ungeschützte öffentliche Netze wie das Internet zum Transport der Daten verwendet werden, ohne die Vertraulichkeit oder Integrität der Daten zu gefährden.



Das TAINY xMOD-V3 arbeitet ausschließlich als OpenVPN-Client, der die Verbindung zu einem OpenVPN-Server initiiert. Daher muss der gegenüberliegende Endpunkt einen OpenVPN-Server besitzen, der die Verbindung akzeptiert.

Hinweis

Bitte beachten Sie, dass die OpenVPN-Implementierung im TAINY xMOD-V3 auf die Anmeldung per Username und Passwort unter gleichzeitiger Verwendung eines Server-Zertifikats beschränkt ist. Andere Authentisierungsmethoden werden derzeit nicht unterstützt.

Zur Authentisierung am OpenVPN-Server benötigt das TAINY xMOD-V3 folgende Informationen, die Sie in der Regel vom Administrator des OpenVPN-Servers erhalten:

- feste IP-Adresse oder Domain-Name des OpenVPN-Servers
- Port, über den die OpenVPN-Verbindung aufgebaut werden soll
- Benutzernamen und Passwort für die Anmeldung am OpenVPN-Server
- Root-Server-Zertifikat (Wurzelzertifikat) des OpenVPN-Servers

Anders als beim IPsec-VPN, unterstützt das TAINY xMOD-V3 maximal eine OpenVPN-Verbindung.

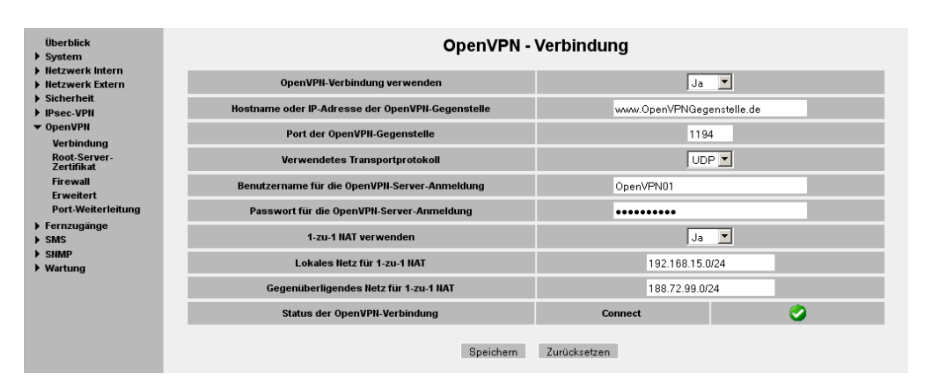
Das TAINY xMOD-V3 authentisiert sich beim OpenVPN-Server durch die vom Administrator des OpenVPN-Servers erhaltene Benutzername/Passwort-Kombination. Bei erfolgreicher Authentifizierung erhält der OpenVPN-Client des TAINY eine eigene IP-Adresse.

Für die Authentisierung des OpenVPN-Servers am TAINY xMOD-V3 muss im TAINY xMOD-V3 das Root-Server-Zertifikat des OpenVPN-Servers installiert sein.

8.2 Verbindungseinstellungen

OpenVPN > Verbindung

NUR TAINY xMOD-V3



Funktion

Richten Sie das TAINY xMOD-V3 gemäß den Absprachen mit dem Systemadministrator der Gegenstelle ein.

OpenVPN-Verbindung verwenden

Aktivieren Sie hier die OpenVPN-Funktion des TAINY xMOD-V3:

Mit *OpenVPN-Verbindung verwenden – Ja* schalten Sie die OpenVPN-Funktion des TAINY xMOD-V3 ein, mit *Nein* wird sie ausgeschaltet.

Nach dem Aktivieren der OpenVPN-Funktion werden Eingabefelder für die Konfiguration der OpenVPN-Verbindung eingeblendet.

Hostname oder IP-Adresse der OpenVPN-Gegenstelle

Geben Sie hier die Adresse der Gegenstelle an, entweder als Host-Namen (z.B. myadress.com) oder als IP-Adresse.

Port der OpenVPN-Gegenstelle

Geben Sie hier den Port an, über den die OpenVPN-Verbindung aufgebaut und betrieben werden soll.

Verwendetes Transportprotokoll

Geben Sie hier das Protokoll an, über das die OpenVPN-Verbindung aufgebaut und betrieben werden soll.

OpenVPN kann *TCP* oder *UDP* verwenden.

Benutzername für die OpenVPN-Server-Anmeldung

Tragen Sie hier den Benutzernamen ein, mit dem sich das TAINY xMOD-V3 am OpenVPN-Server anmelden soll.

Passwort für die OpenVPN-Server-Anmeldung	Tragen Sie hier das Passwort ein, mit dem sich das TAINY xMOD-V3 in Kombination mit dem Benutzernamen am OpenVPN-Server anmelden soll.
1-zu-1-NAT verwenden	Das TAINY xMOD-V3 verfügt über eine 1-zu-1-NAT-Funktion zum gegenüberliegenden Netz der OpenVPN-Verbindung.

Hierzu müssen folgende Informationen bekannt sein (vom Mobilfunkanbieter bzw. -vertragspartner zu beziehen):

- *IP-Adresse des gegenüberliegenden Netzes* und die
- *Netzmaske des gegenüberliegenden Netzes*

Ist 1-zu-1-NAT abgeschaltet, müssen lokale Applikationen diesen Adressbereich zur Adressierung von Gegenstellen im gegenüberliegenden Netz der OpenVPN-Verbindung verwenden.

Ist 1-zu-1-NAT aktiviert, kann ein lokal verwendeter Adressbereich definiert werden, über den lokale Applikationen Gegenstellen im gegenüberliegenden Netz der OpenVPN-Verbindung adressieren können.

Die 1-zu-1-NAT-Funktion im TAINY xMOD-V3 bildet dann den lokal definierten Adressbereich des gegenüberliegenden Netzes (*Lokales Netz für 1-1 NAT*) auf den tatsächlichen Adressbereich des gegenüberliegenden Netzes (*Gegenüberliegendes Netz für 1-zu-1 NAT*) der OpenVPN-Verbindung ab.

Nein	Das TAINY xMOD-V3 verwendet kein 1-zu-1-NAT zum gegenüberliegenden Netz der OpenVPN-Verbindung.
Ja	Das TAINY xMOD-V3 verwendet 1-zu-1-NAT zum gegenüberliegenden Netz der OpenVPN-Verbindung.

1-zu-1 NAT verwenden	Ja
Lokales Netz für 1-zu-1 NAT	192.168.15.0/24
Gegenüberligendes Netz für 1-zu-1 NAT	188.72.99.0/24

Lokales Netz für 1-zu-1-NAT	Tragen Sie hier die IP-Adresse samt Netzmaske ein, über die vom lokalen Netz des TAINY xMOD-V3 auf das gegenüberliegende Netz der OpenVPN-Verbindung zugegriffen werden soll. Verwenden Sie hierzu das CIDR-Format (siehe Kapitel 16). Beispiel: 192.168.15.0/24
Gegenüberliegendes Netz für 1-zu-1-NAT	Tragen Sie hier die tatsächliche Adresse des gegenüberliegenden Netzes der OpenVPN-Verbindung ein. Sie erhalten diese Information von Ihrem Mobilfunkbetreiber bzw. -vertragspartner. Geben Sie die Adresse im CIDR-Format an (siehe Kapitel 16). Beispiel: 188.72.99.0/24
Status der OpenVPN-Verbindung	In *Status der OpenVPN-Verbindung* wird der jeweilige Zustand der OpenVPN-Verbindung angezeigt. Es gibt die folgenden Zustände:

Init	Der OpenVPN-Dienst wird initialisiert.
WAN Waiting	Das TAINY hat noch keine IP-Adresse vom externen Netzwerk bezogen. OpenVPN kann noch keine Verbindung aufbauen.
Configuring	Die Konfiguration für die OpenVPN-Verbindung wird aus der Konfigurationsdatei ausgelesen, geprüft und geladen.
Connecting	Das TAINY versucht aktuell eine OpenVPN-Verbindung aufzubauen.
Connect	Die OpenVPN-Verbindung ist erfolgreich aufgebaut.
Delaying	Das TAINY hat Probleme beim Aufbau der OpenVPN-Verbindung und ist in das unter *Wartezeit zwischen den*

Verbindungsversuchen zur Gegenstelle festgelegte Intervall eingetreten (siehe auch 8.5).

Zusätzlich zum Statustext wird über ein Symbol angezeigt, ob eine OpenVPN-Verbindung etabliert ist

 Die OpenVPN-Verbindung ist erfolgreich aufgebaut

 Es ist keine VPN-Verbindung aufgebaut

8.3 Root-Server-Zertifikat

OpenVPN > Root-Server-Zertifikat



Funktion

Um die Authentizität des gewählten OpenVPN-Servers zu überprüfen, benötigt das TAINY xMOD-V3 eine Kopie des im OpenVPN-Server hinterlegten Root-Server-Zertifikats. Diese Kopie muss vor dem ersten Verbindungsaufbau im TAINY xMOD-V3 installiert sein.

Root-Server-Zertifikat auswählen

Wählen Sie hier das für die Verbindung zum OpenVPN-Server benötigte Root-Server-Zertifikat aus und spielen Sie es mit *Laden* in das TAINY xMOD-V3 ein.

Zertifikatname

Nach dem erfolgreichen Einspielen des Root-Server-Zertifikats wird hier der Name des Zertifikats angezeigt.

Hinweis

Es kann nur ein Root-Server-Zertifikat zurzeit im Gerät hinterlegt werden.

Hinweis

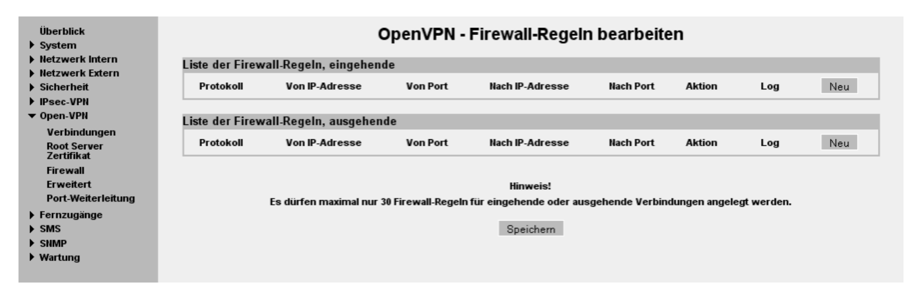
Root-Server-Zertifikate können überschrieben, aber nicht gelöscht werden. Zum Überschreiben wählen Sie ein neues Zertifikat aus und installieren es im Gerät. Das bisherige Zertifikat wird dabei ersetzt.

8.4 Firewall-Regeln für OpenVPN-Verbindung

OpenVPN > Firewall

NUR TAINY xMOD-V3

Unter OpenVPN > Firewall können Firewall-Regeln für die OpenVPN-Verbindung eingerichtet werden:



OpenVPN –Firewall-Regeln bearbeiten

Werkseitig ist der Datenverkehr durch den OpenVPN-Tunnel blockiert. Sie können den Datenverkehr jedoch gezielt durch Anlegen von entsprechenden Firewall-Regeln erlauben.

Gehen Sie bei der Einrichtung der Firewall-Regeln für die OpenVPN-Verbindung vor, wie bei der Einrichtung der Paketfilter-Funktion der allgemeinen Firewall (siehe Kapitel 6.1).

Die hier festgelegten Regeln gelten ausschließlich für die OpenVPN-Verbindung.

Werkseinstellung

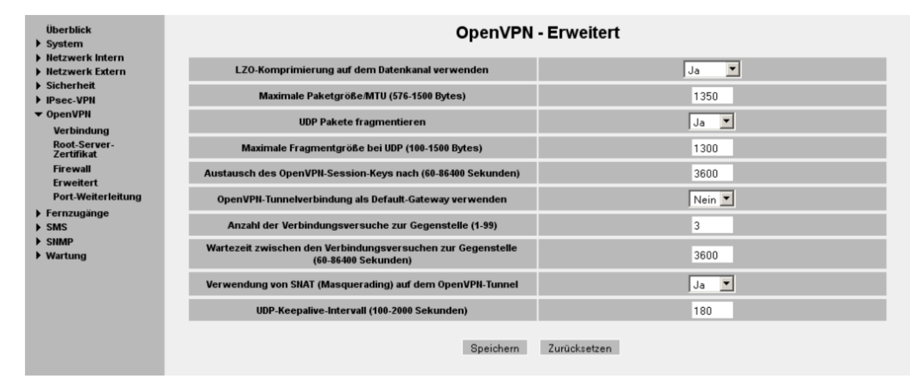
Werkseitig verwendet das TAINY xMOD-V3 folgende Einstellungen für eine neu angelegte Verbindung (eingehend und ausgehend):

Protokoll	**Alle**
Von IP-Adresse	**0.0.0.0/0**
Von Port	**ANY**
Nach IP-Adresse	**0.0.0.0/0**
Nach Port	**ANY**
Aktion	**Verwerfen**
Log	**Nein**

8.5 Erweiterte Einstellungen der OpenVPN-Verbindung

OpenVPN > Erweitert

NUR TAINY xMOD-V3



Funktion

Stellen Sie hier die folgenden Wartezeiten, Intervalle, Paketgrößen und Zusatzfunktionen für die OpenVPN-Verbindung ein.

LZO-Komprimierung auf dem Datenkanal verwenden

Legen Sie hier fest, ob die Daten auf der OpenVPN-Verbindung nach dem LZO-Algorithmus (Lempel-Ziv-Oberhumer-Algorithmus) komprimiert werden sollen.

Mit *Ja*, wird die LZO-Kompression aktiviert, mit *Nein* deaktiviert.

Maximale Paketgröße (MTU)

Die *MTU* beschreibt die maximale Größe der Pakete, die über die OpenVPN-Verbindung gesendet werden können. Größere Pakete müssen intern in Segmentteile zerlegt werden.

Die Maximale Paketgröße (MTU) ist von 576 bis 1500 Bytes einstellbar.

UDP-Pakete fragmentieren

Schalten Sie hier die Fragmentierung von UDP-Paketen ein oder aus. Je nach Einstellung wird das Format des UDP-Headers angepasst.

Nein — UDP-Pakete werden nicht fragmentiert, sie besitzen keine Fragmentierungs-Bytes im Header.

Ja — UDP-Pakete werden gegebenenfalls fragmentiert, sie besitzen in jedem Fall vier Fragmentierungs-Bytes im Header.

Maximale Fragmentgröße für UDP	Der Parameter *Maximale Fragmentgröße für UDP* gibt die maximale Paketgröße (Schwelle) an, die bei Verwendung des UDP-Protokolls erlaubt ist. Größere Pakete müssen in Segmentteile (Fragmente) zerlegt werden. Die *Maximale Fragmentgröße für UDP* ist von 100 bis 1500 Bytes einstellbar.
Austausch des OpenVPN-Session-Keys nach () Sekunden	Mit diesem Parameter wird das Zeitintervall festgelegt, in dem die verwendeten Sitzungsschlüssel einer bestehenden OpenVPN-Verbindung automatisch erneuert werden. Sitzungsschlüssel dienen zur Ver- und Entschlüsselung von Datenpaketen. Das Zeitintervall ist von 60s bis 86400s einstellbar.
OpenVPN-Tunnel-verbindung als Default-Gateway verwenden	Wird die OpenVPN-Tunnelverbindung als Default-Gateway eingestellt, werden alle Pakete, die aus dem lokalen Netz an eine dem TAINY unbekannte IP-Adresse gehen, an die OpenVPN-Verbindung weitergeleitet. Bei *Ja* ist die OpenVPN-Verbindung als Standard-Gateway gesetzt, bei *Nein* nicht.
Anzahl der Verbindungsversuche zur Gegenstelle	Schlägt der Verbindungsversuch zu einem OpenVPN-Server fehl, wird der Vorgang entsprechend dem hier festgelegten Wert wiederholt. Anschließend geht das TAINY in einen Wartezustand, bevor es erneut die hier festgelegte Anzahl an Versuchen startet. Der Wertebereich liegt bei 1 bis 99 Versuchen.
Wartezeit zwischen den Verbindungs-versuchen zur Gegenstelle (Sekunden)	Nachdem die oben parametrierte Anzahl an Fehlversuchen erreicht wurde, wartet das TAINY xMOD-V3 das hier eingestellte Intervall (in Sekunden) ab, bevor es erneut Versucht, eine OpenVPN-Verbindung aufzubauen. Der gültige Wertebereich für diesen Parameter liegt bei 60 bis 86400 Sekunden.
Verwendung von SNAT (Masquerading) auf dem OpenVPN-Tunnel	Mit diesem Parameter lässt sich das SNAT (Source Network Address Translation) für OpenVPN-Verbindungen aktivieren (zum Thema NAT siehe auch Kapitel 16) Mit *Ja*, wird Source-NAT aktiviert, mit *Nein* deaktiviert.
UDP-Keepalive-Intervall (Sekunden)	Das *UDP-Keepalive-Intervall* legt fest, wie lange Routing-Informationen einer erkannten UDP-Verbindung im TAINY erhalten bleiben, nachdem das letzte Paket über die Verbindung verschickt wurde. Mit jedem weiteren Paket wird das Intervall neu gestartet. Es gilt für alle UDP-Routing-Informationen im TAINY xMOD-V3. Das Zeitintervall ist von 100s bis 2000s einstellbar.

Werkseinstellung

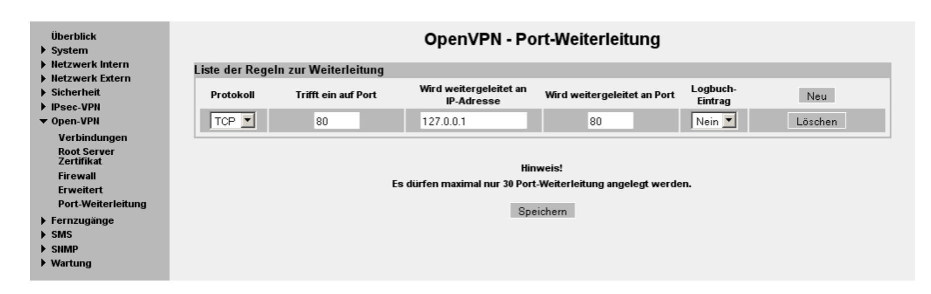
Werkseitig verwendet das TAINY xMOD-V3 folgende Einstellungen:

LZO-Komprimierung auf dem Datenkanal verwenden	**Ja**
Maximale Paketgröße (MTU)	**1350**
Maximale Fragmentgröße für UDP	**1300**
Austausch des OpenVPN-Session-Keys nach () Sekunden	**3600**
OpenVPN-Tunnel-verbindung als Default-Gateway verwenden	**Nein**
Anzahl der Verbindungsversuche zur Gegenstelle	**3**

Wartezeit zwischen den Verbindungs-versuchen zur Gegenstelle (Sekunden)	**3600**
Verwendung von SNAT (Masquerading) auf dem OpenVPN-Tunnel	**Ja**
UDP-Keepalive-Intervall (Sekunden)	**180**

8.6 Port-Weiterleitung

OpenVPN > Port-Weiterleitung



Funktion

Ist hier eine entsprechende Regel zur Port-Weiterleitung erstellt, dann werden Datenpakete, die über die OpenVPN-Verbindung aus dem externen Netz auf einem festgelegten Port des TAINY xMOD eintreffen, an eine festgelegte IP-Adresse und Port-Nummer im lokalen Netz weitergeleitet. Die Port-Weiterleitung kann für TCP oder UDP konfiguriert werden.

Bei Port-Weiterleitung geschieht Folgendes: Der Header eingehender Datenpakete aus dem externen Netz, die über die OpenVPN-Verbindung an die IP-Adresse des OpenVPN-Endpunktes des TAINY xMOD-V3 sowie an einen bestimmten Port gerichtet sind, werden so umgeschrieben, dass sie ins interne Netz an einen bestimmten Rechner und zu einem bestimmten Port dieses Rechners weitergeleitet werden. D.h. die IP-Adresse und Port-Nummer im Header eingehender Datenpakete werden geändert.

Dieses Verfahren wird auch Destination-NAT oder Port Forwarding genannt.

Hinweis

Damit die über die OpenVPN-Verbindung ankommenden Datenpakete an die festgelegte IP-Adresse im lokalen Netz weitergeleitet werden können, muss für diese IP-Adresse eine entsprechende eingehende Firewall-Regel in der OpenVPN-Firewall eingerichtet werden (siehe Kapitel 8.4.)

Neu	Fügt eine neue Weiterleitungs-Regel hinzu, die Sie dann ausfüllen können.
Löschen	Entfernt angelegte Weiterleitungs-Regeln wieder.
Protokoll	Geben Sie hier das Protokoll (TCP oder UDP) an, auf das sich die Regel beziehen soll.
Trifft ein auf Port	Geben Sie hier die Portnummer (z.B. 80) an, auf dem die Datenpakete aus dem externen Netz eintreffen, die weitergeleitet werden sollen.

Wird weiter-geleitet an IP-Adresse	Geben Sie hier die IP-Adresse im lokalen Netz an, an die die eintreffenden Datenpakete weitergeleitet werden sollen.
Wird weiter-geleitet an Port	Geben Sie hier die Nummer des Ports (z.B. 80) an, über den die eintreffenden Datenpakete zur festgelegten IP-Adresse im lokalen Netz weitergeleitet werden sollen.
Logbuch-Eintrag	Für jede einzelne Port-Weiterleitungs-Regel können Sie festlegen, ob bei Greifen der Regel - das Ereignis protokolliert werden soll - *Logbuch-Eintrag* auf *Ja* setzen - oder nicht - *Logbuch-Eintrag* auf *Nein* setzen (Werks-einstellung). Das Protokoll wird in das Firewall-Logbuch, siehe Kapitel 6.5, geschrieben.

Mit *Speichern* werden vorgenommene Änderungen in die Konfiguration des TAINY xMOD-V3 geschrieben.

Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Regeln zur Weiterleitung	**-**
Protokoll	**TCP**
Trifft ein auf Port	**80**
Wird weitergeleitet an IP-Adresse	**127.0.0.1**
Wird weitergeleitet an Port	**80**
Logbuch-Eintrag	**Nein (Ausgeschaltet)**

9 Zugang

9.1 Authentifizierung - Lokal

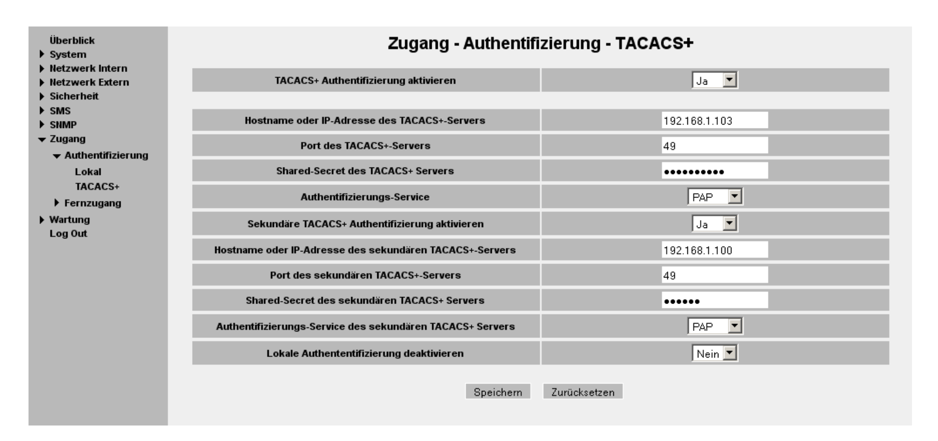
Zugang > Authentifizierung > Lokal



Das Ändern des Zugangspassworts ist in Kapitel 3.9 beschrieben.

9.2 Authentifizierung - TACACS+

Zugang > Authentifizierung > TACACS+



Funktion

Bei der Authentifizierungsmethode TACACS+ (Terminal Access Controller Access Control System Plus) sind die Zugangsdaten für das TAINY xMOD nicht im Gerät selbst, sondern auf einem externen Server hinterlegt.

Bei einer Anmeldeanfrage leitet das TAINY xMOD die erhaltenen Anmeldedaten an den TACACS+-Server weiter. Dieser prüft ihre Gültigkeit und meldet das Ergebnis an das TAINY xMOD zurück, das die Anmeldung daraufhin ablehnt oder akzeptiert.

Aktivieren Sie hier das Authentifizierungsverfahren TACACS+ und legen Sie die Parameter fest, die das TAINY xMOD für eine Verbindung zum TACACS+-Server benötigt.

Sobald der TACACS+-Dienst aktiviert wurde, kann im Anmelde-Fenster des TAINY über ein zusätzliches Aufklappmenü die Art der Anmeldung ausgewählt werden (*TACACS+* oder *Lokal*).

Benutzername	
Passwort	
Authentifizierungsverfahren	TACACS+

Einloggen

Zum Einloggen müssen Cookies in ihrem Browser aktiviert sein.

Hinweis

Benutzer, die sich per TACACS+ am TAINY xMOD anmelden, haben auf Konfigurationsseiten, mit denen sich Zugangsrechte verändern lassen, keinen Zugriff:

- Zugang > Authentifizierung > Lokal
- Wartung > Kommando ausführen
- Wartung > Werkseinstellung

Diese Webseiten stehen ausschließlich lokal angemeldeten Benutzern zur Verfügung.

TACACS+-Authentifizierung aktivieren

Aktivieren bzw. Deaktivieren Sie hier die Authentifizierung per TACACS+.

Nein Die TACACS+-Authentifizierung wird deaktiviert, d.h. es kann sich nur *lokal* an das TAINY xMOD angemeldet werden.

Ja Die TACACS+-Authentifizierung wird aktiviert, d.h. eine Anmeldung am TAINY xMOD kann sowohl *lokal* als auch per TACACS+ erfolgen. Bei Aktivierung werden weitere Eingabefelder angezeigt, über die die Daten zur Anmeldung am TACACS+-Server konfiguriert werden können.

Sekundäre TACACS+-Authentifizierung aktivieren

Mit diesem Parameter kann ein sekundärer TACACS+-Server aktiviert werden, den das TAINY xMOD für die Authentisierung verwendet, sollte der primäre TACACS+-Server nicht erreichbar sein oder die Verwendung des primären TACACS+-Servers aus anderen Gründen fehlschlagen.

Nein Die Verwendung eines sekundären TACACS+-Servers wird deaktiviert, d.h. das TAINY xMOD verwendet ausschließlich den primären. Die Eingabefelder für den sekundären TACACS+-Server werden verborgen.

Ja Die Verwendung eines sekundären TACACS+-Servers wird aktiviert. Bei Aktivierung werden weitere Eingabefelder angezeigt, über die die Daten zur Anmeldung am sekundären TACACS+-Server konfiguriert werden können. Es können die gleichen Parameter wie beim primären TACACS+-Server festgelegt werden.

Hostname oder IP-Adresse des TACACS+-Servers (primär/sekundär)

Geben Sie hier die Adresse des TACACS+-Servers bzw. des sekundären TACACS+-Servers an, entweder als Host-Namen (z.B. myadress.com) oder als IP-Adresse.

Port des TACACS+-Servers (primär/sekundär)

Hier wird der Port eingetragen, über den Anmeldeanfragen an den TACACS+-Server bzw. sekundären TACACS+-Server abgesetzt werden müssen.

Shared Secret des TACACS+-Servers (primär/sekundär)

Dieser Parameter enthält ein geheimes Kennwort, mit dem der Datentransfer zum TACACS+-Server bzw. sekundären TACACS+-Server verschlüsselt wird. Es muss mit dem im korrespondierenden TACACS+-Server hinterlegten Kennwort übereinstimmen.

Authentifizierungs-Service des *TACACS+-Servers*

Mit diesem Parameter wird das Authentifizierungsprotokoll festgelegt, das bei der TACACS+-Anmeldung verwendet wird. Es stehen drei Protokolle zur Auswahl:

(primär/sekundär)

PAP Die Anmeldung wird per PAP (**P**assword **A**uthentication **P**rotokoll) durchgeführt.

CHAP Die Anmeldung wird per CHAP (**C**hallenge **H**andshake **A**uthentication **P**rotocol) durchgeführt.

LOGIN Die Anmeldung findet über eine unverschlüsselte

		Konsolenverbindung (ASCII-Login) statt.
Lokale Authentifizierung deaktivieren	Deaktivieren Sie hier die Möglichkeit, sich per direkter, lokaler Authentifizierung am Gerät anzumelden.	
	Nein	Die Anmeldung am TAINY xMOD ist sowohl über die im TACACS+-Server als auch die direkt im Gerät hinterlegten Anmeldedaten möglich.
	Ja	Die Anmeldung am TAINY xMOD ist ausschließlich über die im TACACS+-Server hinterlegten Anmeldedaten möglich. Auch jeglicher Zugriff per SSH wird bei dieser Einstellung unterbunden.

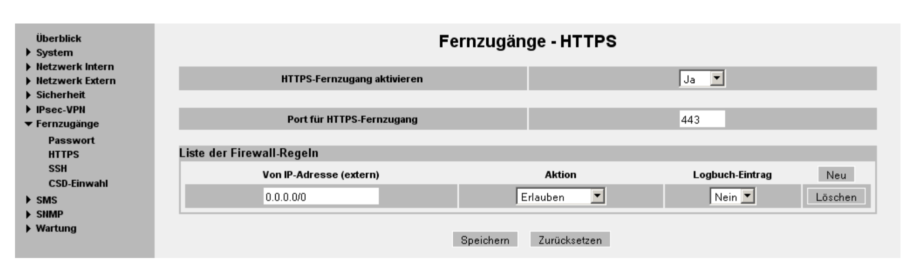
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Einstellung	Wert
TACACS+-Authentifizierung aktivieren	**Nein (Ausgeschaltet)**
Hostname oder IP-Adresse des TACACS+-Servers (primär/sekundär)	**192.168.1.100**
Port des TACACS+-Servers (primär/ sekundär)	**49**
Shared Secret *des TACACS+-Servers* (primär/sekundär)	**secret (verdeckt)**
Authentifizierungs-Service *des TACACS+-Servers* (primär/sekundär)	**PAP**
Sekundäre TACACS+-Authentifizierung aktivieren	**Nein**
Lokale Authentifizierung deaktivieren	**Nein**

9.3 Fernzugang - HTTPS

Zugang > Fernzugang > HTTPS



Funktion	Der HTTPS-Fernzugang (= *HyperText Transfer Protocol Secure*) ermöglicht über HSPA+, UMTS, EGPRS oder GPRS einen gesicherten Zugriff aus einem externen Netz auf die Web-Oberfläche des TAINY xMOD. Die Konfiguration des TAINY xMOD über den HTTPS-Fernzugang erfolgt dann genauso wie die Konfiguration per Web-Browser über die lokale Schnittstelle.	
HTTPS-Fernzugang aktivieren	*Ja*	Der Zugriff auf die Web-Oberfläche des TAINY xMOD per HTTPS aus dem externen Netz ist gestattet.
	Nein	Der Zugriff per HTTPS ist nicht gestattet.

Port für HTTPS-Fernzugang

Standard: 443 (Werkseinstellung)

Sie können einen anderen Port festlegen. Wenn Sie jedoch einen anderen Port festgelegt haben, dann muss die externe Gegenstelle, die den Fernzugriff ausübt, bei der Adressenangabe hinter der IP-Adresse die Port-Nummer angeben.

Beispiel:
Ist dieses TAINY xMOD über die Adresse 192.144.112.5 über das Internet zu erreichen, und ist für den Fernzugang die Port-Nummer 442 festgelegt, dann muss bei der externen Gegenstelle im Web-Browser angegeben werden:
https://192.144.112.5:442

Hinweis

Der Standard-Port 443 für den HTTPS-Zugang bleibt neben dem neu gewählten Port offen.

Liste der Firewall-Regeln

Neu — Fügt eine neue Firewall-Regel für den HTTPS-Fernzugang hinzu, die Sie dann ausfüllen können.

Löschen — Entfernt eine angelegte Firewall-Regel für den HTTPS-Fernzugang wieder.

Von IP-Adresse (extern) — Geben Sie hier die Adresse(n) des/der Rechner(s) an, dem/denen Fernzugang erlaubt ist. Bei den Angaben haben Sie folgende Möglichkeiten:

IP-Adresse oder -Adressbereich: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 16.

Aktion — Bestimmen Sie wie bei Zugriffen auf den angegebenen HTTPS-Port verfahren wird:

Erlauben bedeutet, die Datenpakete dürfen passieren.

Zurückweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält.

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verworfen, so dass der Absender keine Information über deren Verbleib erhält.

Logbuch-Eintrag — Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf *Ja* setzen
- oder nicht - *Log* auf *Nein* setzen (werkseitige Voreinstellung)

Das Protokoll wird in das Firewall-Logbuch, siehe Kapitel 6.5, geschrieben.

Werkseinstellung

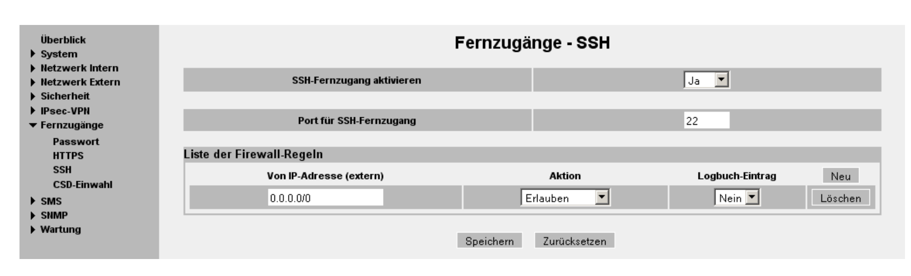
Werkseitig hat das TAINY xMOD folgende Einstellungen:

HTTPS-Fernzugang aktivieren	**Nein (Ausgeschaltet)**
Port für HTTPS-Fernzugang	**443**
Vorgabe für neue Regel:	
Von IP-Adresse (extern)	**0.0.0.0/0**
Aktion	**Erlauben**

Logbuch-Eintrag	**Nein (Ausgeschaltet)**

9.4 Fernzugang - SSH

Zugang > Fernzugang > SSH



Funktion

Der SSH-Fernzugang (= *Secured SHell*) ermöglicht über HSPA+, UMTS, EGPRS oder GPRS einen gesicherten Zugriff aus einem externen Netz auf das Dateisystem des TAINY xMOD.

Dazu muss mit einem SSH-fähigen Programm eine Verbindung von der externen Gegenstelle zum TAINY xMOD aufgebaut werden.

Verwenden Sie den SSH-Fernzugang nur, wenn Sie mit dem LINUX-Dateisystem vertraut sind.

Werkseitig ist diese Option ausgeschaltet.

Vorsicht

Über den SSH-Fernzugang ist es möglich, das Gerät so falsch zu konfigurieren, dass es zum Service eingeschickt werden muss. Kontaktieren Sie in diesem Fall bitte Ihren Händler oder Distributor.

Vorsicht

Ist der Parameter *Lokale Authentifizierung deaktivieren* auf der TACACS+-Konfigurations-Webseite auf *Ja* gesetzt, ist ebenfalls der SSH-Zugang zum Gerät deaktiviert (siehe 9.2).

SSH-Fernzugang aktivieren

Ja	Der Zugriff auf das Dateisystem des TAINY xMOD per SSH aus dem externen Netz ist gestattet.
Nein	Der Zugriff per SSH ist nicht gestattet.

Port für SSH-Fernzugang

Standard: 22 (Werkseinstellung)

Sie können hier einen alternativen Port festlegen. Wenn Sie den alternativen Port nutzen wollen, dann muss die externe Gegenstelle, die den Fernzugriff ausübt, bei der Adressenangabe vor der IP-Adresse die Nummer des alternativen Ports angeben.

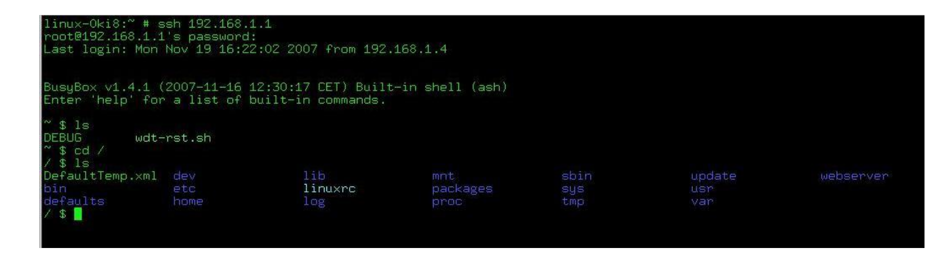
Hinweis

Der Standard-Port 22 für den SSH Zugang bleibt neben dem neu gewählten Port offen.

Beispiel:
Ist dieses TAINY xMOD über die Adresse 192.144.112.5 aus dem externen Netz zu erreichen, und ist für den Fernzugang der Port 22222 festgelegt, dann muss bei der externen Gegenstelle im SSH-Client (z. B. PUTTY) diese Port-Nummer angegeben werden:

ssh -p 22222 192.144.112.5

Beispiel Konsole:



Liste der Firewall-Regeln		
	Neu	Fügt eine neue Firewall-Regel für den SSH-Fernzugang hinzu, die Sie dann ausfüllen können.
	Löschen	Entfernt eine angelegte Firewall-Regel für den SSH-Fernzugang wieder.
	Von IP-Adresse (extern)	Geben Sie hier die Adresse(n) des/der Rechner(s) an, dem/denen Fernzugang erlaubt ist. Bei den Angaben haben Sie folgende Möglichkeiten: IP-Adresse oder -Adressbereich: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 16.
	Aktion	Bestimmen Sie wie bei Zugriffen auf den angegebenen SSH-Port verfahren wird: *Erlauben* bedeutet, die Datenpakete dürfen passieren. *Zurückweisen* bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. *Verwerfen* bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verworfen, so dass der Absender keine Information erhält über deren Verbleib.
	Logbuch-Eintrag	Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel - das Ereignis protokolliert werden soll - *Log* auf *Ja* setzen - oder nicht - *Log* auf *Nein* setzen (werkseitige Voreinstellung) Das Protokoll wird in das Firewall-Logbuch, siehe Kapitel 6.5 geschrieben.

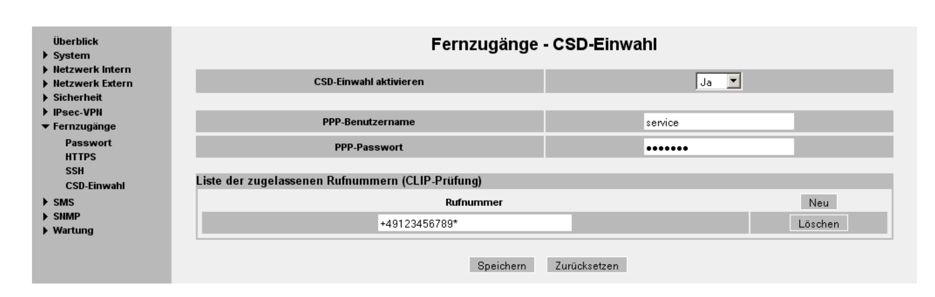
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

SSH-Fernzugang aktivieren	**Nein (Ausgeschaltet)**
Port für SSH-Fernzugang	**22**
Vorgabe für neue Regel:	
Von IP-Adresse (extern)	**0.0.0.0/0**
Aktion	**Erlauben**
Logbuch-Eintrag	**Nein (Ausgeschaltet)**

9.5 Fernzugang über Wählverbindung

Zugang > Fernzugang > CSD-Einwahl



Funktion

Der Zugang CSD-Einwahl ermöglicht den Zugriff auf die Web-Oberfläche und SSH-Konsole des TAINY xMOD über eine Daten-Wählverbindung (*CSD = Circuit Switched Data*). Rufen Sie dazu das TAINY xMOD mit einem analogen Modem auf der Datenrufnummer oder mit einem GSM-Modem auf der Sprach- oder Datenrufnummer seiner SIM-Karte an. Das TAINY xMOD nimmt den Ruf an, wenn

- die Rufnummer des Telefonanschlusses von dem aus Sie den Anruf tätigen in der Liste der zugelassenen Nummern im TAINY xMOD gespeichert ist und
- die Rufnummer vom Telefonnetz übertragen wird (CLIP-Funktion)

Die Einwahl muss mit einem PPP-Client erfolgen, zum Beispiel über eine DFÜ-Verbindung unter Windows. Folgen Sie unter Windows dem *Assistenten für neue Verbindungen* und richten Sie als *Verbindung mit dem Netzwerk am Arbeitsplatz* eine *DFÜ-Verbindung* ein.

Web-Oberfläche und SSH-Konsole haben bei CSD-Einwahl die IP-Adresse 10.99.99.1.

Hinweis

Beim TAINY HMOD ist diese Funktion nur verfügbar, wenn ein GSM-Netz verwendet wird. In UMTS-Netzen, kann diese Funktion nicht verwendet werden.

CSD-Einwahl aktivieren

Ja — Der Zugriff auf dasTAINY xMOD per Daten-Wählverbindung ist gestattet.

Nein — Der Zugriff per Daten-Wählverbindung ist nicht gestattet.

PPP-Benutzername / PPP-Passwort

Wählen Sie einen Benutzernamen und ein Passwort aus, mit dem sich ein PPP-Client (z.B. DFÜ-Verbindung unter Windows) am TAINY xMOD anmelden muss. Den gleichen Benutzernamen und das gleiche Passwort müssen Sie beim PPP-Client eintragen.

Liste der zugelassenen Rufnummern (CLIP-Prüfung)	Geben Sie die *Rufnummer* des Telefonanschlusses an, von dem aus die Daten-Wählverbindung aufgebaut wird. Der Telefonanschluss muss die Rufnummernübermittlung (CLIP – Calling Line Identification Presentation) unterstützen und die Funktion muss eingeschaltet sein.

Die im TAINY xMOD eingetragene Rufnummer muss exakt mit der gemeldeten Rufnummer übereinstimmen und gegebenenfalls auch die Länderkennung und Vorwahl umfassen, z.B. +494012345678.

Wenn mehrere Rufnummern einer Nebenstellenanlage zugangsberechtigt sein sollen, können sie das Zeichen „*“ als Joker verwenden, z.B. +49401234*. Alle Rufnummern die mit +49401234 beginnen werden dann akzeptiert.

Hinweis

Firewall-Regeln, die für den HTTPS- bzw. SSH-Zugang eingetragen sind, gelten auch für den CSD-Zugang. Als Quell-IP-Adresse (*„von IP*“) für den CSD-Zugang ist 10.99.99.2 festgelegt.

Neu	Fügt eine neue zugelassene Rufnummer für den CSD-Fernzugang hinzu, die Sie dann ausfüllen können.
Löschen	Entfernt eine Rufnummer für den CSD-Fernzugang wieder.

Werkseinstellung

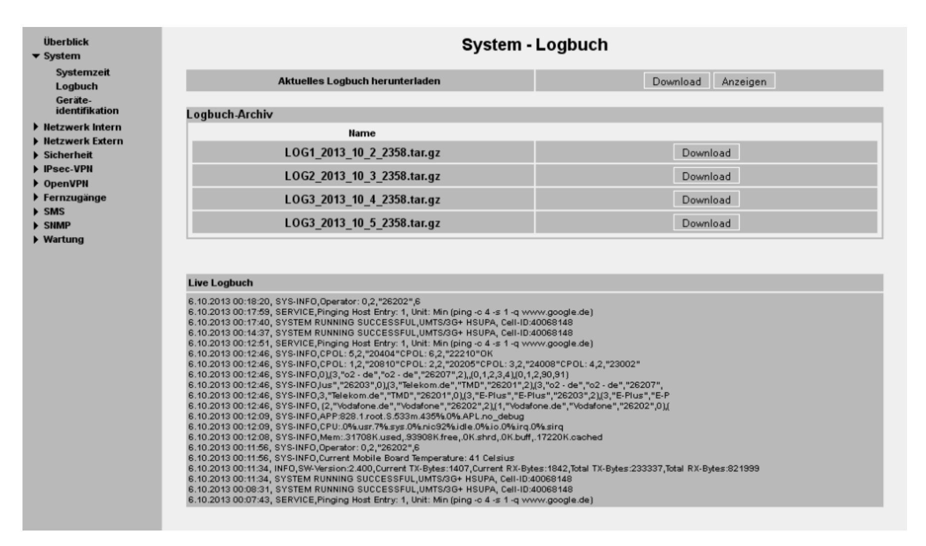
Werkseitig hat das TAINY xMOD folgende Einstellungen:

CSD-Einwahl aktivieren	**Nein (Ausgeschaltet)**
PPP-Benutzername	**service**
PPP-Passwort	**service**
Liste der zugelassenen Rufnummern (CLIP-Prüfung)	*****

10 Logbuch, Update und Diagnose

10.1 Anzeige Logbuch

System > Logbuch



Logbuch

Im Logbuch werden wichtige Ereignisse im Betriebsablauf des TAINY xMOD abgespeichert:

- Neustart
- Änderungen der Konfiguration
- Verbindungsaufbau
- Verbindungsunterbrechungen
- Signalstärke
- Speicher- und CPU-Auslastung
- u.v.m.

Das Logbuch wird bei Erreichen einer Dateigröße von 1MByte, spätestens aber nach 24 Stunden im Logbuch Archiv des TAINY xMOD gespeichert.

Aktuelles Logbuch herunterladen

Download - das aktuelle Logbuch wird auf den Admin-PC geladen. Sie können das Verzeichnis auswählen, in dem die Datei auf dem Admin-PC gespeichert wird und die Datei dort betrachten.

Logbuch-Archiv

Download - archivierte Logbuch-Dateien werden auf den Admin-PC geladen. Sie können das Verzeichnis auswählen, in dem die Dateien auf dem Admin-PC gespeichert werden und die Dateien dort betrachten.

Hinweis

Im Gegensatz zum aktuellen Logbuch liegen die Logbuch-Dateien aus dem Logbuch-Archiv in einem gepackten Format (*tar.gz) vor. Zum Betrachten des Logbuchs öffnen Sie die Logbuch-Datei in einem geeigneten Pack-Programm und klicken sich durch die Ordnerstruktur. Das eigentliche Logbuch hat den Dateinamen *current.log*.

Beispiel:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=---	STAT=---	COPS=---	17	SWC	80		Starting Switch Supervision							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=---	STAT=---	COPS=---	4	GSML	53	GSM STARTING								
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=---	STAT=---	COPS=---	17	KERUP	80		Kernel Version: Linux 2.6.35.3-dnt-0.53.872 #1 Thu Aug 9 11:04:57 CEST 2012 armv5tejl							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=---	STAT=---	COPS=---	4	DNSH	69	SERVICE	DNS: Using Provider defined Peer DNS Server(s)							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=---	STAT=---	COPS=---	4	DNSH	69	SERVICE	Current Peer DNS: 10.74.210.210 ...							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=---	STAT=---	COPS=---	4	GSML	53	GSM STARTING	Start Connection with SIM Card Slot 1							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=0	STAT=0	COPS=---	4	GSML	54	MOBILE MODULE CONNECT	Start Powering Mobile							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=0	STAT=0	COPS=---	4	APL	0	SYSTEM STARTING	Hardware-ID:01-026							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=0	STAT=0	COPS=---	4	APL	0	SYSTEM STARTING	Software-ID:02-021							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=0	STAT=0	COPS=---	4	APL	0	SYSTEM STARTING	Product-Name:TAINY HMOD-V3-E5DS							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=0	STAT=0	COPS=---	4	APL	0	SYSTEM STARTING	MAC Address Eth0:00:25:69:62:1A:C8							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=0	STAT=0	COPS=---	4	APL	0	SYSTEM STARTING	MAC Address Eth1:00:25:69:62:1B:C8							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=0	STAT=0	COPS=---	4	APL	0	SYSTEM STARTING	Success							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=0	STAT=0	COPS=---	4	GSML	55	MOBILE POWER ON								
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=0	STAT=0	COPS=---	4	GSML	56	PIN REQUESTING	Mobile on and Powered successful	wait for PIN Ready or PIN Required						
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=0	STAT=0	COPS=---	4	GSML	58	PIN REQUIRED	PIN Required	Send PIN to Mobile						
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=0	STAT=0	COPS=---	4	GSML	57	PIN READY	PIN Ready							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=10	STAT=1	COPS=26201	4	GSML	61	WAN CONNECTION	Deny Roaming (Network:Auto UMTS Prefered).	Using only Operator:26201						
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=10	STAT=1	COPS=26201	4	GSML	61	WAN CONNECTION	Roaming Mode: Deny Roaming	use only current Provider from SIM Card	Success					
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=10	STAT=1	COPS=26201	4	GSML	61	WAN CONNECTION	Network roaming prohibited	current Network:26201						
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=10	STAT=1	COPS=26201	4	GSML	61	WAN CONNECTION	Mobile Module:PH8		Ok					
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=10	STAT=1	COPS=26201	4	GSML	60	GSM ATTACH	Network Attaching: Attempt:1:Max:10							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=10	STAT=1	COPS=26201	4	GSML	60	GSM ATTACH	Network Attach Success							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=14	STAT=1	COPS=26201	4	GSML	61	WAN CONNECTION	Dialing to Network	Connect Attempt:1	Max:3					
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=14	STAT=1	COPS=26201	4	GSML	61	WAN CONNECTION	WAN Connect	Wait for IP Allocation						
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=14	STAT=1	COPS=26201	4	GSML	61	WAN CONNECTION	Current Peer DNS: 10.74.210.210 ...							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=14	STAT=1	COPS=26201	4	GSML	8	IP ASSIGNED	31.250.75.139							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=14	STAT=1	COPS=26201	4	APL	3	WAN CONNECTION ESTABLISHED	Network Connect stable							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=14	STAT=1	COPS=26201	4	DNSH	69	SERVICE	DNS: Using Provider defined Peer DNS Server(s)							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=14	STAT=1	COPS=26201	4	DNSH	69	SERVICE	Current Peer DNS: 10.74.210.210 ...							
6.10.2012 15:14	TAINY HMOD-V3-E5DS	CSQ=11	STAT=1	COPS=26201	4	APL	34	SYSTEM RUNNING SUCCESSFUL	UMTS	3G	Cell:7941273	Version:-	TXS:299	RXS:530	TX:390992	RX:825330
6.10.2012 15:19	TAINY HMOD-V3-E5DS	CSQ=11	STAT=1	COPS=26201	4	APL	34	SYSTEM RUNNING SUCCESSFUL	UMTS	3G	Cell:7941273	Version:-	TXS:299	RXS:530	TX:390992	RX:825330
6.10.2012 15:24	TAINY HMOD-V3-E5DS	CSQ=14	STAT=1	COPS=26201	4	APL	34	SYSTEM RUNNING SUCCESSFUL	UMTS	3G	Cell:7941273	Version:-	TXS:299	RXS:530	TX:390992	RX:825330
6.10.2012 15:29	TAINY HMOD-V3-E5DS	CSQ=11	STAT=1	COPS=26201	4	APL	34	SYSTEM RUNNING SUCCESSFUL	UMTS	3G	Cell:7941273	Version:-	TXS:299	RXS:530	TX:390992	RX:825330

Einträge im Logbuch

Spalte A: Zeitstempel

Spalte B: Dr. Neuhaus Produktkennung

Spalte C: Signalqualität (CSQ-Wert)

Spalte D: GSM-Einbuchstatus

STAT = --- = Funktion noch nicht gestartet

STAT = 1 = Im Heimatnetz eingebucht

STAT = 2 = Nicht eingebucht; Netzsuche

STAT = 3 = Einbuchen abgelehnt

STAT = 5 = Eingebucht in Fremdnetz (Roaming)

Spalte E: Angabe der Identifikation des Netzbetreibers mit dem 3-stelligen Ländercode (MCC) und dem 2-3-stelligen Netzbetreibercode (MNC).

Beispiel: 26201 (262 = Ländercode / 01 = Netzbetreibercode)

Spalte F: Kategorie des Logbuch-Meldung (für Kundendienst)

Spalte G: Interne Quelle des Logbuch-Meldung (für Kundendienst)

Spalte H: Interne Meldungsnummer (für Kundendienst)

Spalte I: Logbuch-Meldung im Klartext

Spalten J-Q: Zusatzinformationen zur Klartextmeldung, wie zum Beispiel:

- Cell-ID (Identifikationsnummer der aktiven GSM-Zelle)
- Softwareversion
- TXS, RXS (Übertragene IP-Pakete der aktuellen Verbindung)
- TX, RX (Übertragene IP-Pakete seit letztem Werksneustart)

Live-Logbuch

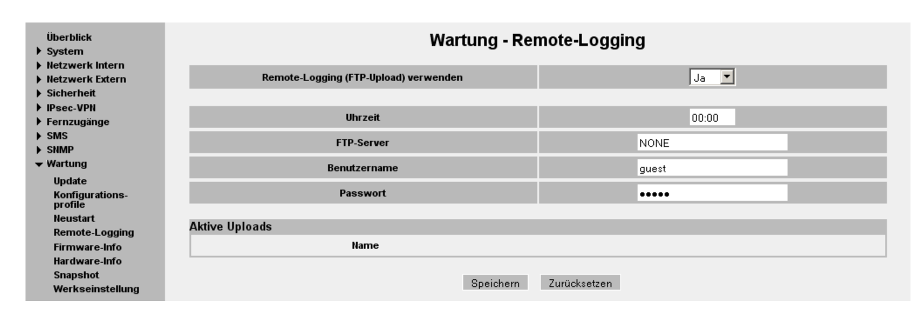
Das *Live-Logbuch* zeigt die neuesten 20 Logbuch-Einträge samt Zeitstempel an. Es aktualisiert sich automatisch und dient dem schnellen Überblick über den Zustand und das Verhalten des Systems.

Live Logbuch

```
6.10.2013 00:18:20, SYS-INFO,Operator: 0,2,"26202",6
6.10.2013 00:17:59, SERVICE,Pinging Host Entry: 1, Unit: Min (ping -c 4 -s 1 -q www.google.de)
6.10.2013 00:17:40, SYSTEM RUNNING SUCCESSFUL,UMTS/3G+ HSUPA, Cell-ID:40068148
6.10.2013 00:14:37, SYSTEM RUNNING SUCCESSFUL,UMTS/3G+ HSUPA, Cell-ID:40068148
6.10.2013 00:12:51, SERVICE,Pinging Host Entry: 1, Unit: Min (ping -c 4 -s 1 -q www.google.de)
6.10.2013 00:12:46, SYS-INFO,CPOL: 5,2,"20404"CPOL: 6,2,"22210"OK
6.10.2013 00:12:46, SYS-INFO,CPOL: 1,2,"20810"CPOL: 2,2,"20205"CPOL: 3,2,"24008"CPOL: 4,2,"23002"
6.10.2013 00:12:46, SYS-INFO,0),(3,"o2 - de","o2 - de","26207",2),,(0,1,2,3,4),(0,1,2,90,91)
6.10.2013 00:12:46, SYS-INFO,lus","26203",0),(3,"Telekom.de","TMD","26201",2),(3,"o2 - de","o2 - de","26207",
6.10.2013 00:12:46, SYS-INFO,3,"Telekom.de","TMD","26201",0),(3,"E-Plus","E-Plus","26203",2),(3,"E-Plus","E-P
6.10.2013 00:12:46, SYS-INFO, (2,"Vodafone.de","Vodafone","26202",2),(1,"Vodafone.de","Vodafone","26202",0),(
6.10.2013 00:12:09, SYS-INFO,APP:828.1.root.S.533m.435%.0%.APL.no_debug
6.10.2013 00:12:09, SYS-INFO,CPU:.0%.usr.7%.sys.0%.nic92%.idle.0%.io.0%.irq.0%.sirq
6.10.2013 00:12:08, SYS-INFO,Mem:.31708K.used,.93908K.free,.0K.shrd,.0K.buff,.17220K.cached
6.10.2013 00:11:56, SYS-INFO,Operator: 0,2,"26202",6
6.10.2013 00:11:56, SYS-INFO,Current Mobile Board Temperature: 41 Celsius
6.10.2013 00:11:34, INFO,SW-Version:2.400,Current TX-Bytes:1407,Current RX-Bytes:1842,Total TX-Bytes:233337,Total RX-Bytes:821999
6.10.2013 00:11:34, SYSTEM RUNNING SUCCESSFUL,UMTS/3G+ HSUPA, Cell-ID:40068148
6.10.2013 00:08:31, SYSTEM RUNNING SUCCESSFUL,UMTS/3G+ HSUPA, Cell-ID:40068148
6.10.2013 00:07:43, SERVICE,Pinging Host Entry: 1, Unit: Min (ping -c 4 -s 1 -q www.google.de)
```

10.2 Remote-Logging

Wartung > Remote-Logging



Funktion

Das TAINY xMOD kann das System-Logbuch einmal am Tag per FTP (= File Transfer Protocol) an einen FTP-Server übertragen.

Übertragen wird das aktuelle System-Logbuch sowie die System-Log-Dateien im Archiv. Nach erfolgreicher Übertragung werden die übertragenen System-Logbücher im TAINY xMOD gelöscht.

Schlägt die Übertragung fehl, versucht das TAINY xMOD nach 24 Stunden erneut die Daten zu übertragen.

Hinweis

Nach fehlgeschlagenem FTP-Upload werden die Logfiles unter Wartung > Remote-Logging in der Liste „Aktive Uploads“ abgelegt.

Remote-Logging (FTP-Upload) verwenden	Mit *Ja* wird die Funktion eingeschaltet.
Uhrzeit	Legt die *Uhrzeit* fest, zu der die Logbücher übertragen werden sollen.
FTP-Server	Legt die Adresse des *FTP-Servers* fest, zu dem die Log-Dateien übertragen werden sollen. Die Adresse kann als Host-Name (z.B. ftp.server.de) oder als IP-Adresse angegeben werden.
Benutzername	Legt den Benutzernamen für die Anmeldung am FTP-Server fest.
Passwort	Legt das Passwort für die Anmeldung am FTP-Server fest.
Aktive Uploads	In dieser Liste werden diejenigen Log-Dateien angezeigt, die aufgrund eines fehlgeschlagenen FTP-Uploads nicht korrekt übermittelt werden konnten. Das TAINY xMOD versucht, diese Dateien beim nächsten FTP-Upload erneut zu übermitteln.

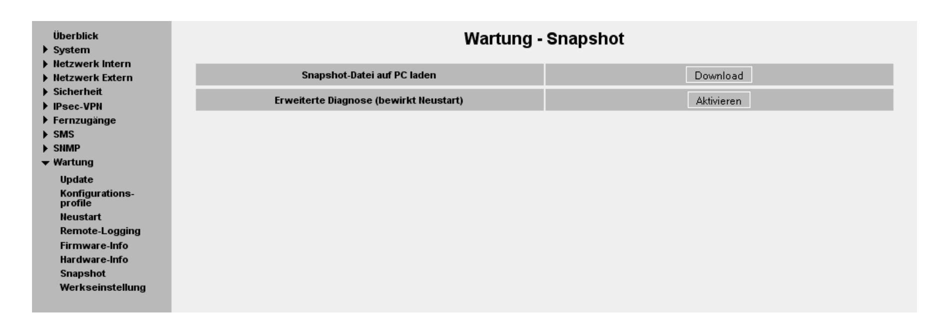
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Remote-Logging (FTP-Upload) verwenden	**Nein (Ausgeschaltet)**
Uhrzeit	**00:00**
FTP-Server	**NONE**
Benutzername	**guest**
Passwort	**guest**

10.3 Snapshot

Wartung > Snapshot



Funktion

Diese Funktion dient Support-Zwecken.

Der Service-Snapshot speichert wichtige Logdateien und aktuelle Geräte-Einstellungen, die zur Fehlerdiagnose relevant sein könnten in einer Datei.

Wenn Sie sich bei einem Problem mit dem TAINY xMOD an unseren Kundendienst wenden, wird dieser in vielen Fällen um die Snapshot-Datei bitten.

Hinweis

Diese Datei enthält die Zugangsparameter zum Datenfunkdienst (HSPA+, UMTS, EGPRS oder GPRS) sowie die Adressen der Gegenstelle. Nicht enthalten sind Benutzername und Passwort für den Zugang zum TAINY xMOD.

Snapshot-Datei auf PC laden

Klicken Sie auf *Download*. Sie können auswählen, an welche Stelle auf dem Admin-PC die Snapshot-Datei gespeichert werden soll.

Der Dateiname der Snapshot-Datei setzt sich folgendermaßen zusammen:

<hostname>_Snapshot_<Date&TimeCode>.tgz,

z.B.: tainyHMOD_Snapshot_200711252237.tgz

Erweiterte Diagnose (bewirkt Neustart)

Die *Erweiterte Diagnose* hilft bei einer gezielten Problemanalyse. *Aktivieren* Sie bitte die e*rweiterte Diagnose* nur nach Aufforderung durch unseren Kundendienst. Bei aktivierter erweiterter Diagnose werden zusätzliche Informationen in die Diagnose-Logbücher geschrieben, was zu einem erhöhten Datenaufkommen und vermehrtem Schreibzugriff auf den nicht-flüchtigen Speicher im Gerät führt.

Bei Aktivierung der *Erweiterten Diagnose* führt das TAINY xMOD automa-tisch einen Neustart aus.

Hinweis

Durch die häufigen Schreibzugriffe bei aktivierter *erweiterter Diagnose* auf den nicht-flüchtigen Speicher des TAINY xMOD kann sich dessen Lebensdauer verringern.

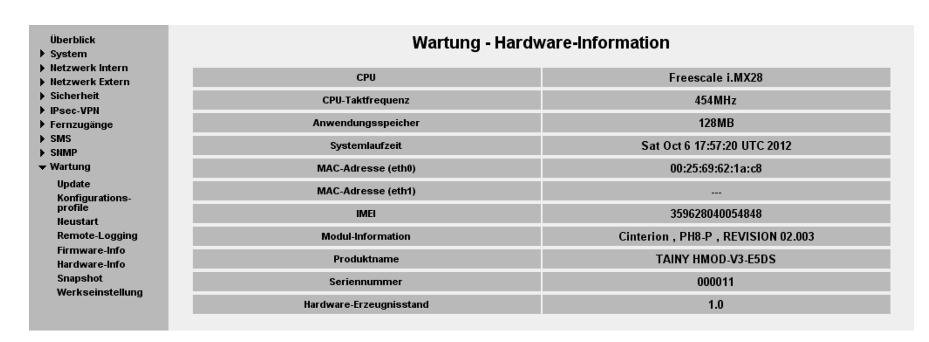
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Erweiterte Diagnose	**Aktivieren (Zustand: Aus)**

10.4 Hardware-Informationen

Wartung > Hardware-Info

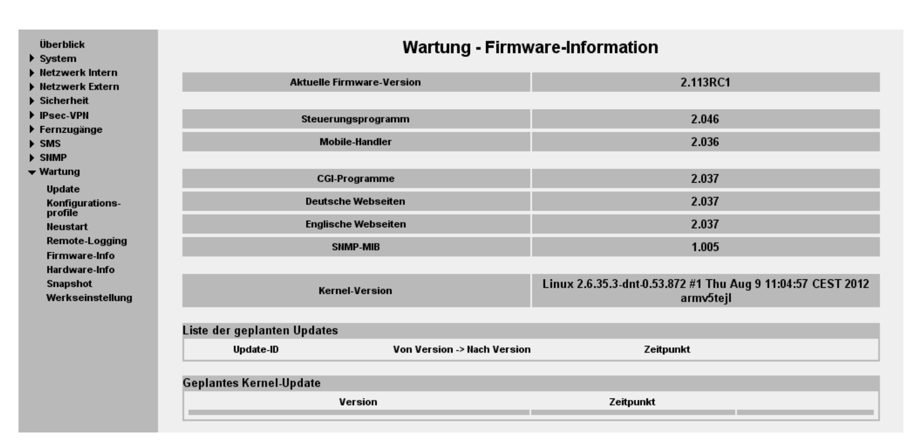


Funktion

Anzeige wichtiger Informationen zur Hardware-Identifikation. Bei Anfragen an unseren Kundendienst werden diese Informationen in vielen Fällen benötigt.

10.5 Firmware-Informationen

Wartung > Firmware-Info



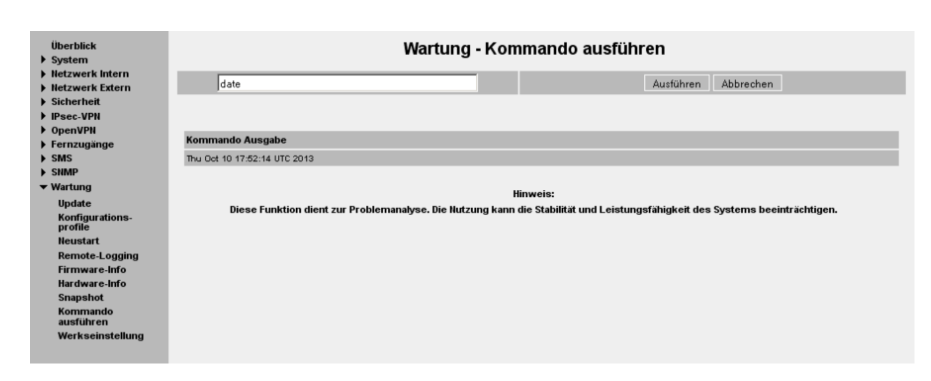
Funktion

Anzeige wichtiger Informationen zur Firmware-Identifikation. Bei Anfragen an unseren Kundendienst werden diese Informationen in vielen Fällen benötigt.

Zusätzlich werden geplante Firmware- und Kernel-Updates angezeigt. Siehe auch Kapitel 10.7.

10.6 Kommando ausführen

Wartung > Kommando ausführen



Funktion

Über die Funktion *Kommando ausführen* können Linux-Kommandozeilen-befehle an das TAINY abgesetzt werden. Das TAINY führt diese direkt aus und zeigt ihre Ergebnisse unter *Kommando-Ausgabe* an.

Vorsicht

Diese Funktion dient ausschließlich der Problemanalyse. Durch unvorsichtige Nutzung kann die Stabilität und Leistungsfähigkeit des Systems beeinträchtigt werden. Es ist möglich, das Gerät mit Linux-Befehlen so falsch zu konfigurieren, dass es zum Service eingeschickt werden muss. Kontaktieren Sie in diesem Fall bitte Ihren Händler oder Distributor.

Ausführen Der eingegebene Befehl wird an das TAINY abgesetzt.

Abbrechen Das Befehlseingabefeld und die *Kommando-Ausgabe* werden gelöscht.

10.7 Firmware- und System-Update

Wartung > Update



Funktion

Mit der Update-Funktion können Sie eine neue Betriebssoftware (Firmware) bzw. ein neues System (Kernel und Treiber) in das TAINY xMOD laden und diese Software-Komponenten aktivieren.

Bei einem sofortigen Update wird zunächst das neue Software-Paket (Firmware oder Kernel) entpackt. Dieser Vorgang kann einige Minuten dauern. Danach beginnt der eigentliche Update-Vorgang, der durch ein Lauflicht der S-, Q- und C-LEDs angezeigt wird.

Die bisherigen Einstellungen des TAINY xMOD werden übernommen, sofern diese Einstellungen mit dem neuen Software-Stand noch gültig sind.

Firmware-Update-Zeitpunkt aktivieren

Nein Update sofort - Die neue Firmware wird direkt nachdem Sie die Firmware-Datei ausgewählt und auf die Schaltfläche *Absenden* geklickt haben geladen und aktiviert.

Ja Update zeitgesteuert - Die neue Firmware wird zu dem festgelegten Update-Zeitpunkt aktiviert. Dazu muss die Firmware-Datei zuvor geladen werden.

Firmware-Update-Zeitpunkt festlegen

Wenn Sie das Firmware-Update zeitgesteuert durchführen lassen wollen, geben Sie hier den Zeitpunkt an, an dem die neue Firmware aktiviert werden soll.

Geben Sie *Jahr – Monat – Tag – Stunde – Minute* an.

Firmware-Update-Datei auswählen

Wählen Sie mit *Durchsuchen* die neue Firmware-Datei aus. Eine Firmware-Update-Datei für das TAINY xMOD trägt zum Beispiel folgende Bezeichnung:

EMOD_v2_008_v2_113.tgz

Laden Sie die Firmware mit *Öffnen* in das Gerät.

Absenden

Mit *Absenden* (oberer Button) wird die Firmware entweder sofort oder bei zeitgesteuertem Update zum vorgegeben Zeitpunkt aktiviert.

Zurücksetzen	Mit *Zurücksetzen* (oberer Button) werden alle Firmware-Update-Einstellungen wieder zurückgesetzt, sofern der Firmware-Update-Vorgang noch nicht mit *Absenden* angestoßen wurde.
System-Update-Zeitpunkt aktivieren	*Nein* — Update sofort - Das neue System wird direkt nachdem Sie die System-Update-Datei ausgewählt und auf die Schaltfläche *Absenden* geklickt haben geladen und aktiviert.
	Ja — Update zeitgesteuert - Das neue System wird zu dem festgelegten Update-Zeitpunkt aktiviert. Dazu muss die System-Update-Datei zuvor geladen werden.
System-Update-Zeitpunkt festlegen	Wenn Sie das System-Update zeitgesteuert durchführen lassen wollen, geben Sie hier den Zeitpunkt an, an dem der neue Kernel und die im Paket enthaltenen Treiber aktiviert werden sollen.
	Geben Sie *Jahr – Monat – Tag – Stunde – Minute* an.
System-Update-Datei auswählen	Wählen Sie mit *Durchsuchen* die neue System-Update-Datei aus. System-Update-Datei für das TAINY xMOD trägt zum Beispiel folgende Bezeichnung:
	- **tainy_system_package_update_all_1.0.tgz**
	Laden Sie die System-Update-Datei mit *Öffnen* in das Gerät.
Absenden	Mit *Absenden* (unterer Button) wird das neue System entweder sofort oder bei zeitgesteuertem Update zum vorgegeben Zeitpunkt aktiviert.
Zurücksetzen	Mit *Zurücksetzen* (unterer Button) werden alle System-Update-Einstellungen wieder zurückgesetzt, sofern der System-Update-Vorgang noch nicht mit *Absenden* angestoßen wurde.

11 SMS-Versand

11.1 Einleitung

TAINY xMOD nutzt den Short Message Service (SMS) des GSM.

Unter *Netzwerk Extern - UMTS/EDGE* (TAINY HMOD) bzw. *Netzwerk Extern - EDGE/GPRS* (TAINY EMOD) können Sie ein spezielles SMS-Center definieren (siehe 5.1).

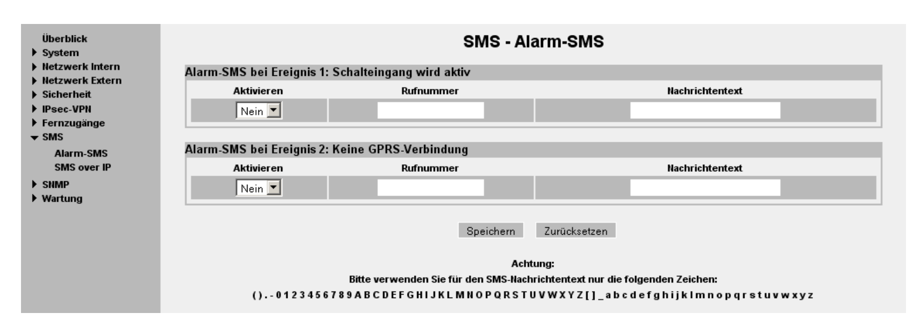
Damit die SMS-Funktion sicher funktioniert, tragen Sie dort die Rufnummer des Service-Centers ein, andernfalls wird das Standard-SMS-Center Ihres Netzbetreibers verwendet.

Achtung:

Wird keine Rufnummer für das SMS-Center eingetragen oder erfolgt der Eintrag nicht in internationalem Format (z.B. +49…) kann der SMS-Versand scheitern.

11.2 Alarm-SMS

SMS > Alarm-SMS



Funktion	Das TAINY xMOD kann kurze Alarm-Meldungen über den SMS (= Short Message Service) des GSM-Netzes versenden. Zwei Ereignisse können den Versand einer Alarm-Meldung über SMS auslösen: - Ereignis 1: Schalteingang wird aktiv - Ereignis 2: Keine UMTS- bzw. GPRS-Verbindung Zu jedem der beiden Ereignisse kann eine eigene Rufnummer angegeben werden, an die die Alarm-Meldung geschickt wird. Ebenso kann der Text der Alarm-Meldung frei festgelegt werden.
Alarm-SMS bei Ereignis 1: Schalteingang wird aktiv	Der Schalteingang wechselt von inaktiv auf aktiv, d.h. am Schalteingang wird eine ausreichende Schaltspannung angelegt. Diese Funktion kann zum Beispiel genutzt werden, um außerhalb der IP-Datenverbindungen Alarm-Meldungen der lokalen Applikationen zu versenden.
Alarm-SMS bei Ereignis 2: Keine GPRS-Verbindung	Die Verbindung zum Datenfunkdienst (HSPA+, UMTS, EGPRS, GPRS) kommt trotz mehrfacher Versuche nicht zustande. Das TAINY xMOD versendet daraufhin eine Alarm-Meldung.

Einstellungen	*Aktivieren*	Bei *Ja* wird bei Eintreffen des entsprechenden Ereignisses die Alarm-Meldung abgesendet, bei *Nein* nicht.
	Rufnummer	Tragen Sie hier die Rufnummer des Endgerätes ein, an das die Alarm-Meldung über SMS gesendet werden soll. Das Endgerät muss SMS-Empfang über GSM oder Festnetz unterstützen.

Nachrichtentext — Tragen Sie hier den Text ein, der als Alarm-Meldung verschickt werden soll. Es stehen folgende Zeichen zur Verfügung:

, * ' # % = < > ! & + - / ? ( ) . : ; 0 1 2 3 4 5 6 7 8 9
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
a b c d e f g h i j k l m n o p q r s t u v w x y z (+ Leerzeichen)

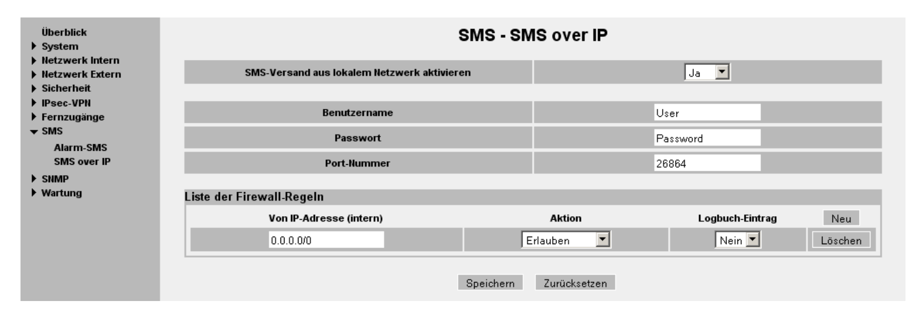
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Alarm-SMS Ereignis 1: Schalteingang wird aktiv	
Aktivieren	**Nein (Ausgeschaltet)**
Rufnummer	**-**
Nachrichtentext	**-**
Alarm-SMS Ereignis 2: : Keine GPRS-Verbindung	
Aktivieren	**Nein (Ausgeschaltet)**
Rufnummer	**-**
Nachrichtentext	**-**

11.3 SMS-Versand aus dem lokalem Netzwerk

SMS > SMS over IP



Funktion

Mit der Funktion *SMS over IP* können Anwendungen, die an der lokalen Schnittstelle des TAINY xMOD angeschlossen sind, über das GSM-Netz Short Messages (SMS) verschicken.

Zum Versand einer SMS muss die Anwendung an der lokalen Schnittstelle eine TCP/IP-Verbindung zum TAINY xMOD aufbauen.

Über diese TCP/IP-Verbindung sendet die Anwendung den Text der SMS an das TAINY xMOD, welches den Text in eine SMS verpackt und diese verschickt.

Format auf der TCP/IP-Verbindung

Der Text muss in folgendem Format über die TCP/IP-Verbindung an das TAINY xMOD übermittelt werden:

Benutzername#Passwort#CommandCode#Seq-Num;Rufnummer;Nachricht

Beispiel: benutzer#passwort#105#01;0049043465789;Mein SMS-Text:

Benutzername

Der Benutzername zur Prüfung der Berechtigung zum Senden einer SMS. Maximal dürfen 10 Zeichen verwendet werden.

Passwort

Das Passwort zur Prüfung der Berechtigung zum Senden einer SMS. Maximal dürfen 10 Zeichen verwendet werden.

CommandCode

Kommando zum SMS-Versand aus dem lokalen Netz. Dieser Wert ist fest 105 und darf nicht verändert werden.

Seq-Num

Die Sequenznummer dient der Zuordnung mehrerer Anfragen gleichzeitig. Die Funktion wird derzeit nicht unterstützt.

Die Sequenznummer besteht aus 2 numerischen Zeichen zwischen 01 bis 99

Rufnummer

Rufnummer des SMS-Empfängers. Die Rufnummer darf 40 Zeichen nicht übersteigen. Internationale Nummern (+49...) sind zulässig.

Nachricht

SMS Text. Der Text darf 160 Zeichen nicht übersteigen. Es stehen folgende Zeichen zur Verfügung:

, * ' % = < > ! & + - / ? ( ) . 0 1 2 3 4 5 6 7 8 9
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
a b c d e f g h i j k l m n o p q r s t u v w x y z (+ Leerzeichen)

Folgende Zeichen haben eine besondere Bedeutung und dürfen im SMS-Text nicht vorkommen:

#	Trennungszeichen der ersten Kommandoebene
;	Trennungszeichen der zweiten Kommandoebene
:	Bestimmt das Ende der Nachricht

SMS-Versand aus lokalem Netzwerk aktivieren	Wählen Sie *Ja* um SMS aus dem lokalen Netzwerk versenden zu können.
Benutzername	Benutzername, der im Nachrichten-Rahmen enthalten sein muss, bevor deren Text per SMS versendet wird. Maximal dürfen 10 Zeichen verwendet werden.
Passwort	Passwort, das im Nachrichten-Rahmen enthalten sein muss, bevor deren Text per SMS versendet wird. Maximal dürfen 10 Zeichen verwendet werden.
Port-Nummer	TCP/IP-Port auf dem das TAINY xMOD die TCP/IP-Verbindung zum SMS-Versand entgegen nimmt.
Liste der Firewall-Regeln	Damit die TCP/IP-Verbindung zum SMS-Versand aufgebaut werden kann, muss am TAINY xMOD eine Firewall-Regel eingerichtet werden. Es können mit *Neu* mehrere Quellen (*Von IP-Adresse (intern)*) für die TCP/IP-Verbindung zum SMS-Versand eingerichtet werden. Mit *Löschen* können Sie Verbindungen wieder entfernen.

Von IP-Adresse (intern)	Legen Sie hier fest, für welchen Client oder welche Gruppe von Clients aus dem lokal ans TAINY xMOD angeschlossene Netzwerk die Firewall-Regel gelten soll. Geben Sie dazu eine entsprechende IP-Adresse oder einen IP-Bereich aus dem lokalen Netz an. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 16. Der Wert 0.0.0.0/0 bedeutet: alle Adressen.
Aktion	Wählen Sie Aktionen, um eine TCP/IP-Verbindung für den SMS-Versand zu erlauben oder zu unterbinden: *Erlauben* bedeutet, die Datenpakete dürfen passieren. *Zurückweisen* bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. *Verwerfen* bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verworfen, so dass der Absender keine Information erhält über deren Verbleib.
Logbuch-Eintrag	Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel - das Ereignis protokolliert werden soll - *Log* auf *Ja* setzen - oder nicht - *Log* auf *Nein* setzen (werkseitige Voreinstellung) Das Protokoll wird in das Firewall-Logbuch geschrieben - siehe Kapitel 6.5.

Werkseinstellung

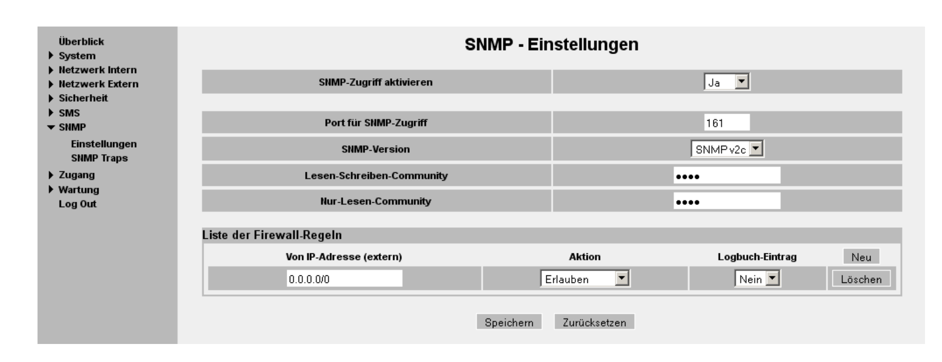
Werkseitig hat das TAINY xMOD folgende Einstellungen:

SMS-Versand aus lokalem Netzwerk aktivieren	**Nein**
Benutzername	**User**
Passwort	**Password**
Port-Nummer	**26864**
Liste der Firewall-Regeln	**Nicht aktiv**
Von IP-Adresse (intern)	**0.0.0.0/0**
Aktion	**Erlauben**
Logbuch-Eintrag	**Nein**

12 SNMP

12.1 Bedienung per SNMP

SNMP > Einstellungen



Verschiedene Parameter des TAINY xMOD können Mithilfe des SNMP (Simple Network Management Protocol) v2c oder v3 abgefragt oder geändert werden. SNMP v3 bietet dabei die umfangreichsten Sicherheitsmechanismen. Der Zugriff per SNMP kann sowohl aus dem lokalen Netz als auch vom externen Netz erfolgen.

Folgende SNMP-Anfragen und -Antworten werden vom TAINY xMOD unterstützt:

GET, GETNEXT, GETBULK, GETSUBTREE, WALK, SET, RESPONSE, TRAP.

Auf die folgenden Parameter des TAINY xMOD kann per SNMP lesend zugegriffen werden:

- Geräteidentifikations-Zeilen (1-4)
- IP-Adresse des externen Netzwerks
- PIN
- MAC-Adresse der lokalen Schnittstelle
- Kennung des aktuellen Mobilfunkbetreibers
- APN
- IMSI
- IMEI
- Signalqualität (CSQ-Wert)
- Signalqualität (dBm-Wert)
- Net-ID
- Cell-ID
- Host-Name
- Maximales Datenvolumen
- Datenvolumen der Warnschwelle 80%
- Aktuell verbrauchtes Datenvolumen (Monatsvolumen)
- Hardware-ID
- Softwareversion
- ICCID (Seriennummer der verwendeten SIM-Karte)
- Access Technology (2G/3G)

Folgende Parameter des TAINY xMOD können per SNMP verändert werden:

- Maximales Datenvolumen (Volumenbegrenzung)
- PIN der SIM-Karte
- Geräteidentifikations-Zeilen (1-4)

Die exakte Beschreibung der Parameter wird als MIB (Management Information Base) auf der Webseite von Dr. Neuhaus (www.neuhaus.de) zur Verfügung gestellt. Gehen Sie dort zur Produktseite des TAINY xMOD.

SNMP-Zugriff aktivieren

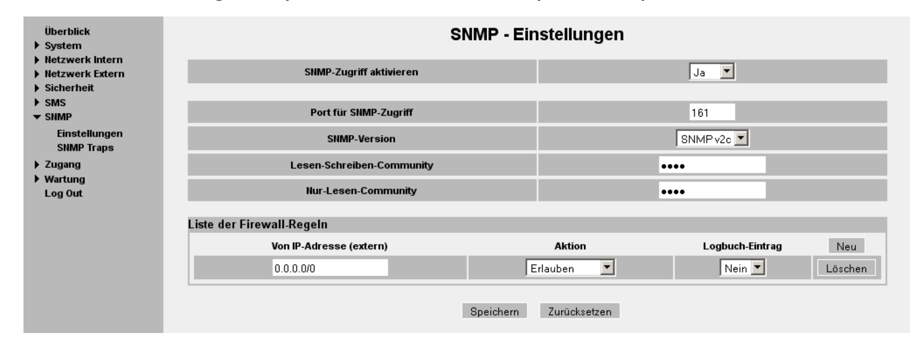
Wählen Sie *Nein*, wenn Sie den SNMP-Zugriff auf das TAINY xMOD sperren wollen.

Wählen Sie *Ja*, wenn Sie den SNMP-Zugriff auf das TAINY xMOD zulassen wollen.

Port für SNMP-Zugriff

Wählen sie den IP-Port aus, über den der SNMP-Zugriff erfolgen soll. Die Werkseinstellung entspricht dem Standard (Port 161).

Bei Verwendung von SNMP v2c



Lesen-Schreiben-Community

Geben Sie die SNMP-Community ein, die lesend und schreibend auf das TAINY xMOD zugreifen darf.

Hinweis

Ändern Sie die Lesen-Schreiben-Community. Die Werkseinstellung ***private*** ist ein Standard-Bezeichner, der allgemein bekannt ist und keine Sicherheit bietet.

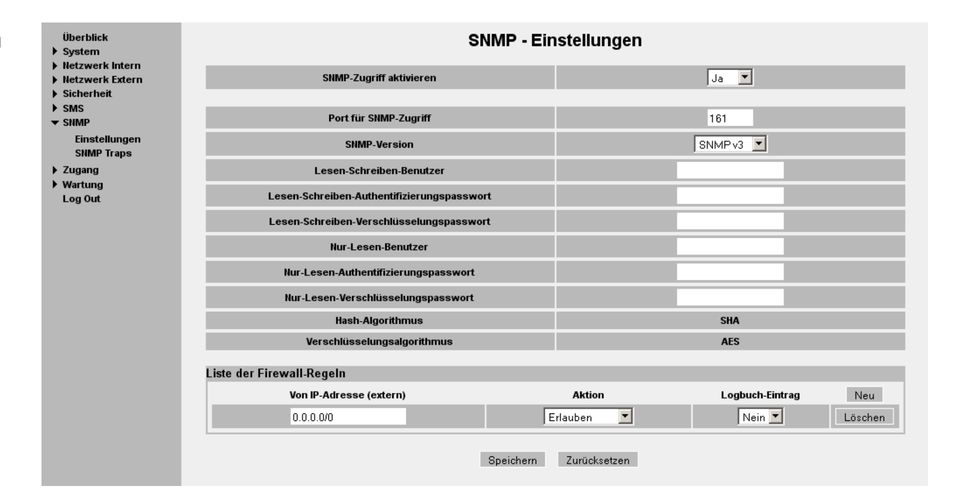
Nur-Lesen-Community

Geben Sie die SNMP-Community ein, die nur lesend auf das TAINY xMOD zugreifen darf.

Hinweis

Ändern Sie die Nur-Lesen-Community. Die Werkseinstellung ***public*** ist ein Standard-Bezeichner, der allgemein bekannt ist und keine Sicherheit bietet.

Bei Verwendung von SNMP v3



Lesen-Schreiben-Benutzer
: Legen Sie hier den Benutzernamen fest, der zur Authentifizierung dient, wenn Parameter des TAINY xMOD sowohl gelesen als auch geschrieben werden dürfen.

Lesen-Schreiben-Authentifizierungs-passwort
: Legen Sie hier das Passwort fest, das zur Authentifizierung dient, wenn Parameter des TAINY xMOD sowohl gelesen als auch geschrieben werden dürfen.

Lesen-Schreiben-Verschlüsselungs-passwort
: Legen Sie hier das Passwort fest, das zur Verschlüsselung dient, wenn Parameter des TAINY xMOD sowohl gelesen als auch geschrieben werden dürfen.

Nur-Lesen-Benutzer
: Legen Sie hier den Benutzernamen fest, der zur Authentifizierung dient, wenn Parameter des TAINY xMOD nur gelesen werden dürfen.

Nur-Lesen-Authentifizierungs-passwort
: Legen Sie hier das Passwort fest, das zur Authentifizierung dient, wenn Parameter des TAINY xMOD nur gelesen werden dürfen.

Nur-Lesen-Verschlüsselungs-passwort
: Legen Sie hier das Passwort fest, das zur Verschlüsselung dient, wenn Parameter des TAINY xMOD nur gelesen werden dürfen.

Hash-Algorithmus
: Zeigt den verwendeten Hash-Algorithmus an. Dieser kann nicht geändert werden.

Verschlüsselungs-Algorithmus
: Zeigt den verwendeten Verschlüsselung-Algorithmus an. Dieser kann nicht geändert werden.

Liste der Firewall-Regeln
: Damit Daten per SNMP ausgetauscht werden können, muss am TAINY xMOD eine Firewall-Regel eingerichtet werden. Es können mit *Neu* mehrere Quellen (*Von IP-Adresse extern*) für die UDP/IP-Verbindung eingerichtet werden. Mit *Löschen* können Sie Verbindungen wieder entfernen.

Von IP-Adresse (extern)
: Tragen Sie die IP-Adresse der externen Gegenstelle ein, für die die Firewall-Regel gelten soll. Geben Sie dazu die IP-Adresse oder einen IP-Bereich der Gegenstelle an. 0.0.0.0/0 bedeutet alle Adressen.

: Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 16.

Aktion
: Wählen Sie Aktionen, um die UDP/IP-Verbindung für SNMP zu erlauben oder zu unterbinden:

: *Erlauben* bedeutet, die Datenpakete dürfen passieren.

: *Zurückweisen* bedeutet, die Datenpakete werden

zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. *Verwerfen* bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verworfen, so dass der Absender keine Information erhält über deren Verbleib.

Logbuch-Eintrag

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf *Ja* setzen
- oder nicht - *Log* auf *Nein* setzen (werkseitige Voreinstellung)

Das Protokoll wird in das Firewall-Logbuch geschrieben - siehe Kapitel 6.5.

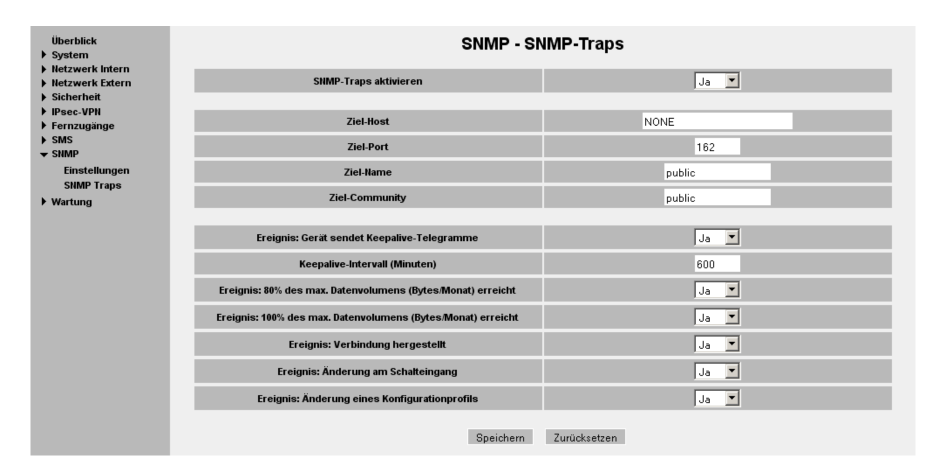
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Einstellung	Wert
SNMP-Zugriff aktivieren	Nein
Port für SNMP-Zugriff	161
Lesen-Schreiben-Community	private
Nur-Lesen-Community	public
Lesen-Schreiben-Benutzer	(leer)
Lesen-Schreiben-Authentifizierungs-passwort	(leer)
Lesen-Schreiben-Verschlüsselungs-passwort	(leer)
Nur-Lesen-Benutzer	(leer)
Nur-Lesen- Authentifizierungs-passwort	(leer)
Nur-Lesen-Verschlüsselungs-passwort	(leer)
Firewall-Regeln	Nicht aktiv
Von IP-Adresse (extern)	0.0.0.0/0
Aktion	Erlauben
Logbuch-Eintrag	Nein

12.2 Alarmmeldungen per SNMP-Traps

SNMP > SNMP-Traps



Das TAINY xMOD versendet Benachrichtigungen in Form von SNMP-Traps bei verschiedenen Ereignissen.

SNMP-Traps aktivieren	Wählen Sie *Ja*, wenn Sie das Versenden von SNMP-Traps aktivieren wollen. Wählen Sie *Nein*, wenn Sie das Versenden von SNMP-Traps ausschalten wollen.
Ziel-Host	Tragen Sie hier die IP-Adresse des SNMP-Trap-Empfängers ein.
Ziel-Port	Tragen Sie hier den IP-Port des SNMP-Trap-Empfängers ein.
Ziel-Name	Tragen Sie hier den Namen des SNMP-Trap-Empfängers ein.
Ziel-Community	Tragen Sie hier die Bezeichnung der SNMP-Community ein.
Ereignis: Gerät sendet Keepalive-Telegramme	Wählen Sie *Ja*, wenn das TAINY xMOD Keepalive-Pakete als SNMP-Trap versenden soll. Wählen Sie *Nein*, wenn das TAINY xMOD keine Keepalive-Pakete als SNMP-Trap versenden soll.
Keepalive-Intervall (Minuten)	Wählen Sie das Intervall mit dem die Keepalive-SNMP-Traps verschickt werden sollen.
Ereignis: 80% des max. Datenvolumens (Bytes/Monat) erreicht	Wählen Sie *Ja*, wenn das TAINY xMOD einen SNMP-Trap bei Erreichen der Warnschwelle (80%) für das monatliche Datenvolumen versenden soll (siehe Kapitel 5.7). Wählen Sie *Nein*, wenn kein SNMP-Trap bei diesem Ereignis versendet werden soll.
Ereignis: 100% des max. Datenvolumens (Bytes/Monat) erreicht	Wählen Sie *Ja*, wenn das TAINY xMOD einen SNMP-Trap bei Erreichen des maximalen monatlichen Datenvolumens versenden soll (siehe Kapitel 5.7) Wählen Sie *Nein*, wenn kein SNMP-Trap bei diesem Ereignis versendet werden soll.
Ereignis: Verbindung wiederhergestellt	Wählen Sie *Ja*, wenn das TAINY xMOD einen SNMP-Trap bei erfolgreicher Wiederherstellung der Verbindung zum APN versenden soll. Wählen Sie *Nein*, wenn kein SNMP-Trap bei diesem Ereignis versendet werden soll.
Ereignis: Änderung am Schalteingang	Wählen Sie *Ja*, wenn das TAINY xMOD einen SNMP-Trap bei einer Änderung am Schalteingang versenden soll. Wählen Sie *Nein*, wenn kein SNMP-Trap bei diesem Ereignis versendet werden soll.

Ereignis: Änderung eines Konfigurations-profils	Wählen Sie *Ja*, wenn das TAINY xMOD einen SNMP-Trap bei einer Änderung an einem Konfigurationsprofil versenden soll. Wählen Sie *Nein*, wenn kein SNMP-Trap bei diesem Ereignis versendet werden soll.

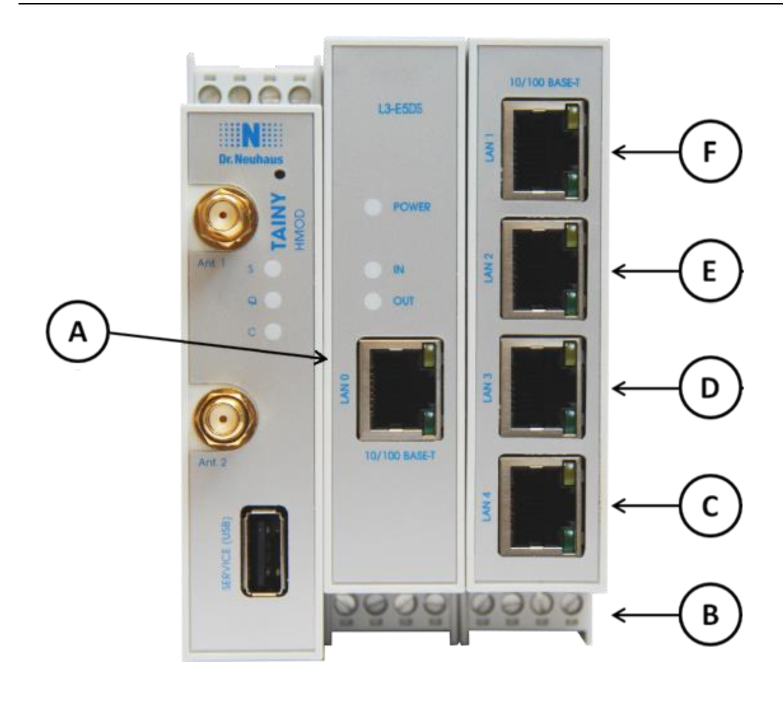
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

SNMP-Traps aktivieren	Nein
Ziel-Host	NONE
Ziel-Port	162
Ziel-Name	public
Ziel-Community	public
Ereignis: Gerät sendet Keepalive-Telegramme	Ja
Keepalive-Intervall (Minuten)	600
Ereignis: 80% des max. Datenvolumens (Bytes/Monat) erreicht	Ja
Ereignis: 100% des max. Datenvolumens (Bytes/Monat) erreicht	Ja
Ereignis: Verbindung hergestellt	Ja
Ereignis: Änderung am Schalteingang	Ja
Ereignis: Änderung eines Konfigurationsprofils	Ja

13 Produktvariante E5 (5-Port-Ethernet-Switch)

13.1 Überblick



A – LAN0 / 10/100-Base-T - RJ45-Buchse mit integrierten Signalleuchten

B – 4 Anschlussklemmen - Reserviert für zukünftige Anwendungen

C – LAN4 / 10/100-Base-T - RJ45-Buchse mit integrierten Signalleuchten

D – LAN3 / 10/100-Base-T - RJ45-Buchse mit integrierten Signalleuchten

E - LAN2 / 10/100-Base-T - RJ45-Buchse mit integrierten Signalleuchten

F – LAN1 / 10/100-Base-T - RJ45-Buchse mit integrierten Signalleuchten

NUR Geräte der Produktvariante E5

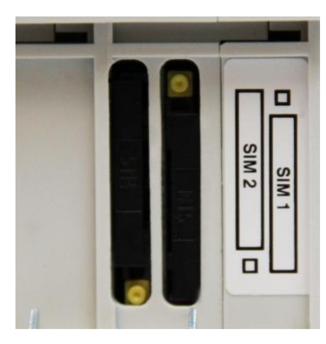
Funktion

TAINY xMOD der Produktvariante E5 (5-Port-Ethernet-Switch) besitzen einen 5-Port-Ethernet-Switch. Die fünf Schnittstellen sind gleichberechtigt. Sie können bspw. zum Anschluss mehrerer Applikationen oder zur lokalen Parametrierung des TAINY xMOD verwendet werden.

14 Produktvariante DS (Dual SIM-Card)

14.1 Überblick

NUR Geräte der Produktvariante DS



Funktion

Geräte der Produktvariante Dual SIM-Card (DS) sind mit einem zweiten SIM-Karteneinschub ausgestattet, der es ermöglicht, eine Verbindung zum Datenfunkdienst (HSPA+, UMTS, EGPRS oder GPRS) alternativ über eine zweite SIM-Karte herzustellen. Diese kann bspw. von einem anderen Provider sein, der beim Ausfall des ersten Providers die Erreichbarkeit des TAINY xMOD sicherstellt.

Dabei gilt:

- Beide SIM-Karten-Einschübe sind gleichberechtigt
- Es ist immer nur jeweils eine SIM-Karte aktiv
- Die Auswahl der SIM-Karten erfolgt über Konfigurationsprofile, die jeweils einem SIM-Karteneinschub fest zugeordnet sind, bzw. die aktuelle Konfiguration des Geräts
- Es ist möglich, einem SIM-Karteneinschub mehrere Konfigurations-profile zuzuweisen
- Die Umschaltzeit zwischen den SIM-Karten-Einschüben hängt im Wesentlichen von den Einwahlzeiten der verwendeten Provider ab. Im Idealfall ist ein Wechsel in unter 50s zu erreichen.

Über die Parametrierung kann festgelegt werden, welches Konfigurations-profil das TAINY xMOD bei einem Geräteneustart aktivieren soll und somit, mit welcher SIM-Karte per Default eine UMTS- bzw. EDGE-/GPRS-Verbindung aufgebaut wird.

Parametrierung

Weitere Informationen zur Parametrierung und Umschaltung von Konfigu-rationsprofilen finden sich in Kapitel 15.

15 Profilwechsel

15.1 Überblick

Funktion

Unterschiedliche Konfigurationen eines TAINY xMOD können in verschiedenen Konfigurationsprofilen hinterlegt und je nach Bedarf aktiviert werden.

Zusätzlich zur manuellen Aktivierung von Konfigurationsprofilen, kann das Gerät auch derart parametriert werden, dass bestimmte festgelegte Ereignisse zu einer automatischen Aktivierung eines anderen Profils führen.

Dies ist z.B. hilfreich, wenn ein Gerät keine Verbindung zum Datenfunkdienst (HSPA+, UMTS, EGPRS oder GPRS) herstellen kann. In diesem Fall ist es möglich, ein anderes Profil zu aktivieren, in dem bspw. ein alternativer APN (Access Point Name) oder andere Zugangsdaten für den Provider hinterlegt sind.

NUR Geräte der Produktvariante DS

Geräte der Produktvariante DS (Dual SIM) besitzen darüber hinaus die Möglichkeit, über einen Profilwechsel eine zweite SIM-Karte anzusprechen, so dass im Fehlerfall die Verbindung über einen komplett anderen Provider realisiert werden könnte.

Umschaltereignisse

Das Umschalten von Konfigurationsprofilen kann durch vier parametrierbare Ereignisse ausgelöst werden:

- Verlust oder Nichterreichbarkeit des Datenfunktdienst-Netzes
- Fehlschlagen der Verbindungsprüfung
- Neustart des Geräts
- Umschaltzeitpunkt gemäß eines festgelegten Timings erreicht

15.2 Konfiguration

Im Folgenden findet sich eine Übersicht, wo in der Web-Oberfläche des TAINY xMOD Profilwechsel für die entsprechenden Ereignisse zu konfigurieren sind.

Achtung:

Bei der Parametrierung von Profilwechseln kann nur aus den bereits auf dem TAINY xMOD hinterlegten Konfigurationsprofilen ausgewählt werden. D.h. ein Konfigurationsprofil muss zumindest im Gerät angelegt sein, wenn es als ‚Ziel-Profil' für einen Wechsel angegeben wird, auch wenn die inhaltliche Parametrierung dieses Profils erst später stattfinden sollte.

Verlust oder Nichterreichbarkeit des Datendienstfunk-Netzes

Ein Profilwechsel im Falle des Verlustes oder der Nichterreichbarkeit der Datendienstfunk-Verbindung wird mit dem Parameter *Bei Verbindungsfehler Rückfall auf Profil* auf der Webseite *Netzwerk Extern - UMTS/EDGE* (TAINY HMOD) bzw. *Netzwerk Extern - EDGE/GPRS* (TAINY EMOD) parametriert (siehe 5.1).

Der Parameterwert ***NONE*** deaktiviert diese Funktion

Fehlschlagen der Verbindungsprüfung

Voraussetzung für einen Profilwechsel im Falle einer fehlgeschlagenen Verbindungsprüfung ist

- die Aktivierung der Parameterprüfung (*Prüfen der Verbindung* auf *Ja* setzen),
- die Eingabe mindestens eines *Host-Namens* (*Liste der Ziel-Hosts*) und
- die Auswahl *Anderes Profil aktivieren* für den Parameter *Aktion bei*

	fehlerhafter Verbindung auf der Webseite *Netzwerk Extern - Erweiterte Einstellungen - Prüfen der Verbindung.* Mit dem Parameter *Zu aktivierendes Profil* kann das Konfigurationsprofil festgelegt werden, zu dem im Fehlerfall gewechselt werden soll (siehe 5.2) Der Parameterwert ***NONE*** deaktiviert diese Funktion
Neustart des Gerätes	Das Profil, das bei einem Neustart des Geräts aktiviert wird, wird mit dem Parameter *Startprofil nach einem Neustart* auf der Webseite *Wartung - Konfigurationsprofile* festgelegt (siehe 3.8) Bei Parameterwert ***NONE*** findet kein Profilwechsel statt, das Gerät verwendet die gleiche Konfiguration, die vor dem Neustart aktiv war.
Umschaltzeitpunkt gemäß eines festgelegten Timings erreicht	Ein zeitgesteuerter Profilwechsel wird mit den Parametern *Profilwechsel nach (Minuten)* und *zu Profil* auf der Webseite *Wartung - Konfigurations-profile* festgelegt (siehe 3.8) Der Parameterwert ***NONE*** deaktiviert diese Funktion

16 Kleines Router-Lexikon

1-zu-1-NAT

Bei 1-zu-1-NAT bildet eine Netzwerkkomponente (z.B.-Router) den Adressbereich des einen Netzes in den Adressbereich eines zweiten Netzes ab.

Beispiel Netz 1:
Adressbereich: 123.123.123.xyz
Ziel-Adresse: 123.123.123.**101**

Beispiel Netz 2:
Adressbereich: 234.234.234.xyz
Ziel-Adresse: 234.234.234.101

Netz 1 ⇔ 1-zu-1-NAT Funktion ⇔ Netz 2

Eine Komponente in Netz 1 adressiert eine Komponente in Netz 2 über eine Zieladresse aus dem Adressbereich von Netz 1. Die 1-zu-1-NAT-Funktion bildet die Zieladresse in den Adressbereich von Netz 2 ab. Antworten aus Netz 2 erhalten umgekehrt eine Absenderadresse aus Netz 1.

AES

Advanced Encryption Standard.

Das NIST (National Institute of Standards and Technology) entwickelt in Zusammenarbeit mit Industrie-Unternehmen seit Jahren den AES-Verschlüsselungsstandard. Diese → symmetrische Verschlüsselung soll den bisherigen DES-Standard ablösen. Der AES-Standard spezifiziert drei verschiedene Schlüsselgrößen mit 128, 192 und 256 Bit. 1997 hatte die NIST die Initiative zu AES gestartet und ihre Bedingungen für den Algorithmus bekannt gegeben. Von den vorgeschlagenen Verschlüsselungsalgorithmen hat die NIST fünf Algorithmen in die engere Wahl gezogen; und zwar die Algorithmen MARS, RC6, Rijndael, Serpent und Twofish. Im Oktober 2000 hat man sich für Rijndael als Verschlüsselungsalgorithmus entschieden.

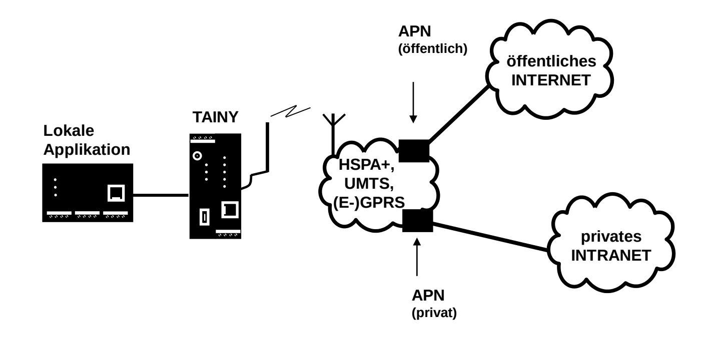
Antennendiversität

Bei aktivierter Antennendiversität wird mittels einer zugeschalteten zweiten Antenne versucht, Störungen und Auslöschungen von Funkwellen, die durch Reflexionen, unterschiedliche Laufzeiten und Überlagerungen auftreten können, zu minimieren. Hierzu werden vom Empfänger die Signale beider Antennen ausgewertet und das als besser erkannte Signal verwendet.

Unter bestimmten Umständen kann es zielführend sein, das Gerät mit nur einer Antenne in Empfangsrichtung zu betreiben. In diesem Fall sollte die Antennendiversität deaktiviert werden.

APN (Access Point Name)

(Zugriffspunktname). Netzübergreifende Verbindungen, z. B. vom Datenfunkdienst (HSPA+, UMTS, EGPRS oder GPRS) ins Internet, werden über so genannte APNs hergestellt.



Ein Endgerät, das eine Verbindung über den Datenfunkdienst aufbauen

will, gibt durch Angabe des APN an, mit welchem Netz es verbunden werden will: Internet oder privates Firmennetz, das über Standleitung angeschlossen ist.

Der APN bezeichnet den Übergabepunkt zum anderen Netz. Er wird dem Benutzer vom Netzbetreiber mitgeteilt.

Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung werden Daten mit einem Schlüssel verschlüsselt und mit einem zweiten Schlüssel wieder entschlüsselt. Beide Schlüssel eignen sich zum Ver- und Entschlüsseln. Einer der Schlüssel wird von seinem Eigentümer geheim gehalten (Privater Schlüssel/Private Key), der andere wird der Öffentlichkeit (Öffentlicher Schlüssel/Public Key), d. h. möglichen Kommunikationspartnern, gegeben.

Eine mit dem öffentlichen Schlüssel verschlüsselte Nachricht kann nur von dem Empfänger entschlüsselt und gelesen werden, der den zugehörigen privaten Schlüssel hat. Eine mit dem privaten Schlüssel verschlüsselte Nachricht kann von jedem Empfänger entschlüsselt werden, der den zugehörigen öffentlichen Schlüssel hat. Die Verschlüsselung mit dem privaten Schlüssel zeigt, dass die Nachricht tatsächlich vom Eigentümer des zugehörigen öffentlichen Schlüssels stammt. Daher spricht man auch von digitaler Signatur, Unterschrift.

Asymmetrische Verschlüsselungsverfahren wie RSA sind jedoch langsam und anfällig für bestimmte Angriffe, weshalb sie oft mit einem symmetrischen Verfahren kombiniert werden (→ symmetrische Verschlüsselung). Andererseits sind Konzepte möglich, die die aufwändige Administrierbarkeit von symmetrischen Schlüsseln vermeiden.

CIDR

Classless InterDomain Routing

IP-Netzmasken und CIDR sind Notationen, die mehrere IP-Adressen zu einem Adressraum zusammenfassen. Dabei wird ein Bereich von aufeinander folgenden Adressen als ein Netzwerk behandelt.

Das CIDR-Verfahren reduziert die z. B. in Routern gespeicherten Routing-Tabellen durch einen Postfix in der IP-Adresse. Mit diesem Postfix können ein Netz und die darunter liegenden Netze zusammengefasst bezeichnet werden. Die Methode ist in RFC 1518 beschrieben. Die nachfolgende Tabelle zeigt links die IP-Netzmaske, ganz rechts die entsprechende CIDR-Schreibweise.

IP-Netzmaske	binär				CIDR
255.255.255.255	11111111	11111111	11111111	11111111	32
255.255.255.254	11111111	11111111	11111111	11111110	31
255.255.255.252	11111111	11111111	11111111	11111100	30
255.255.255.248	11111111	11111111	11111111	11111000	29
255.255.255.240	11111111	11111111	11111111	11110000	28
255.255.255.224	11111111	11111111	11111111	11100000	27
255.255.255.192	11111111	11111111	11111111	11000000	26
255.255.255.128	11111111	11111111	11111111	10000000	25
255.255.255.0	11111111	11111111	11111111	00000000	24
255.255.254.0	11111111	11111111	11111110	00000000	23
255.255.252.0	11111111	11111111	11111100	00000000	22
255.255.248.0	11111111	11111111	11111000	00000000	21
255.255.240.0	11111111	11111111	11110000	00000000	20
255.255.224.0	11111111	11111111	11100000	00000000	19
255.255.192.0	11111111	11111111	11000000	00000000	18
255.255.128.0	11111111	11111111	10000000	00000000	17
255.255.0.0	11111111	11111111	00000000	00000000	16
255.254.0.0	11111111	11111110	00000000	00000000	15
255.252.0.0	11111111	11111100	00000000	00000000	14
255.248.0.0	11111111	11111000	00000000	00000000	13
255.240.0.0	11111111	11110000	00000000	00000000	12

255.224.0.0	11111111	11100000	00000000	00000000	11
255.192.0.0	11111111	11000000	00000000	00000000	10
255.128.0.0	11111111	10000000	00000000	00000000	9
255.0.0.0	11111111	00000000	00000000	00000000	8
254.0.0.0	11111110	00000000	00000000	00000000	7
252.0.0.0	11111100	00000000	00000000	00000000	6
248.0.0.0	11111000	00000000	00000000	00000000	5
240.0.0.0	11110000	00000000	00000000	00000000	4
224.0.0.0	11100000	00000000	00000000	00000000	3
192.0.0.0	11000000	00000000	00000000	00000000	2
128.0.0.0	10000000	00000000	00000000	00000000	1
0.0.0.0	00000000	00000000	00000000	00000000	0

Beispiel: 192.168.1.0 / 255.255.255.0 entspricht im CIDR: 192.168.1.0/24

Um dem TAINY xMOD einen Bereich von IP-Adressen anzugeben z.B. bei der Konfiguration der Firewall, kann es erforderlich sein, den Adressraum in der CIDR-Schreibweise anzugeben.

Client / Server

In einer Client-Server-Umgebung ist ein Server ein Programm oder Rechner, das/der vom Client-Programm oder Client-Rechner Anfragen entgegennimmt und beantwortet.

Bei Datenkommunikation bezeichnet man auch den Rechner als Client, der eine Verbindung zu einem Server (oder Host) herstellt. D.h. der Client ist der anrufende Rechner, der Server (oder Host) der Angerufene.

CSD 9600

CSD (9600) steht für Circuit Switched Data oder Daten-Wählverbindung. Dabei wird eine Verbindung zwischen zwei Teilnehmern (Endpunkten der Verbindung) aufgebaut, ähnlich wie bei einem Telefonat im öffentlichen Fernsprechnetz. Teilnehmer 1 wählt die Rufnummer von Teilnehmer 2. Das Netz signalisiert Teilnehmer 2 den Anruf, Teilnehmer 2 nimmt den Ruf an und das Netz baut die Verbindung auf, bis einer der Teilnehmer die Verbindung wieder beendet.

Im GSM-Netz wird dieser Dienst CSD genannt und erlaubt die Datenübertragung mit 9600 bit/s oder 14400 bit/s, wobei die Übertragung gesichert oder ungesichert stattfindet. Möglich sind Verbindungen GSM Modem zu GSM Modem, Analog Modem zu GSM und ISDN-Modem zu GSM-Modem.

CSQ / RSSI

Der CSQ-Wert ist ein im GSM-Standard festgelegter Wert zur Angabe der Signalqualität. CSQ-Werte korrespondieren zur Empfangsfeldstärke RSSI (= Received Signal Strength Indication):

	RSSI
< 6	< -101 dBm
6 - 10	-101 dBm... - 93 dBm
11 - 18	- 91 dBm... -77 dBm
> 18	> -75 dBm
99	Nicht eingebucht

Datagramm

Beim Übertragungsprotokoll TCP/IP werden Daten in Form von Datenpaketen, den sog. IP-Datagrammen, versendet. Ein IP-Datagramm hat folgenden Aufbau:

1. IP-Header
2. TCP-/UDP-Header
3. Daten (Payload)

Der IP-Header enthält:

- die IP-Adresse des Absenders (source IP address)
- die IP-Adresse des Empfängers (destination IP address)
- die Protokollnummer des Protokolls der nächst höheren Protokollschicht (nach dem OSI-Schichtenmodell)
- die IP-Header Prüfsumme (Checksum) zur Überprüfung der Integrität des Headers beim Empfang.

Der TCP-/UDP-Header enthält folgende Informationen:

- Port des Absenders (source port)
- Port des Empfängers (destination port)
- eine Prüfsumme über den TCP-Header und ein paar Informationen aus dem IP-Header (u. a. Quell- und Ziel-IP-Adresse)

DES / 3DES

Der von IBM stammende und von der NSA überprüfte symmetrische Verschlüsselungsalgorithmus (→ symmetrische Verschlüsselung) DES wurde 1977 vom amerikanischen National Bureau of Standards, dem Vorgänger des heutigen National Institute of Standards and Technology (NIST), als Standard für amerikanische Regierungsinstitutionen festgelegt. Da es sich hierbei um den ersten standardisierten Verschlüsslungsalgorithmus überhaupt handelte, setzte er sich auch schnell in der Industrie und somit außerhalb Amerikas durch.

DES arbeitet mit einer Schlüssellänge von 56Bit, die heute aufgrund der seit 1977 gestiegenen Rechenleistung der Computer als nicht mehr sicher gilt.

3DES ist eine Variante von DES. Es arbeitet mit 3-mal größeren Schlüsseln, die also 168 Bit lang sind. Sie gilt heute noch als sicher und ist unter anderem auch Teil des IPsec-Standards.

DHCP

Dynamic Host Configuration Protocol (DHCP) übernimmt die automatische dynamische Zuweisung von IP-Adressen und weiteren Parametern in einem Netzwerk. Das Dynamic Host Configuration Protocol verwendet UDP. Es wurde definiert im RFC 2131 und bekam die UDP-Ports 67 und 68 zugewiesen. DHCP arbeitet im Client – Server Verfahren, wobei der Client vom Server die IP-Adressen zugewiesen bekommt.

DNS

Die Adressierung in IP-Netzen erfolgt grundsätzlich über IP-Adressen. Bevorzugt wird im Allgemeinen aber die Adressierung in Form einer Domain-Adresse angegeben (d. h. in der Form www.abc.xyz.de). Erfolgt die Adressierung über die Domain-Adresse, sendet der Absender zunächst die Domain-Adresse an einen Domain Name Server (DNS) und erhält die dazugehörige IP-Adresse zurück. Erst dann adressiert der Absender seine Daten an diese IP-Adresse.

DynDNS-Anbieter

Auch *Dynamic DNS-Anbieter*. Jeder Rechner, der mit dem Internet verbunden ist, hat eine IP-Adresse (IP = Internet Protocol). Eine IP-Adresse besteht aus 4 maximal dreistelligen Nummern, jeweils durch einen Punkt getrennt. Ist der Rechner über die Telefonleitung per Modem, per ISDN oder auch per ADSL online, wird ihm vom Internet Service Provider dynamisch eine IP-Adresse zugeordnet, d. h. die Adresse wechselt von Sitzung zu Sitzung. Auch wenn der Rechner (z. B. bei einer Flatrate) über 24 Stunden ununterbrochen online ist, wird die IP-

Adresse zwischendurch gewechselt.

Soll ein lokaler Rechner über das Internet erreichbar sein, muss seine Adresse der externen Gegenstelle bekannt sein. Nur so kann diese die Verbindung zum lokalen Rechner aufbauen. Wenn die Adresse des lokalen Rechners aber ständig wechselt, ist das nicht möglich. Es sei denn, der Betreiber des lokalen Rechners hat einen Account bei einem DynamicDNS-Anbieter (DNS = Domain Name Server).

Dann kann er bei diesem einen Host-Namen festlegen, unter dem der Rechner künftig erreichbar sein soll, z. B.: www.xyz.abc.de. Zudem stellt der DynamicDNS-Anbieter ein kleines Programm zur Verfügung, das auf dem betreffenden Rechner installiert und ausgeführt werden muss. Bei jeder Internet-Sitzung des lokalen Rechners teilt dieses Tool dem DynamicDNS-Anbieter mit, welche IP-Adresse der Rechner zurzeit hat. Dessen Domain Name Server registriert die aktuelle Zuordnung Host-Name - IP-Adresse und teilt diese anderen Domain Name Servern im Internet mit.

Wenn jetzt ein externer Rechner eine Verbindung herstellen will zum lokalen Rechner, der beim DynamicDNS-Anbieter registriert ist, benutzt der externe Rechner den Host-Namen des lokalen Rechners als Adresse. Dadurch wird eine Verbindung hergestellt zum zuständigen DNS (Domain Name Server), um dort die IP-Adresse nachzuschlagen, die diesem Host-Namen zurzeit zugeordnet ist. Die IP-Adresse wird zurück übertragen zum externen Rechner und jetzt von diesem als Zieladresse benutzt. Diese führt jetzt genau zum gewünschten lokalen Rechner.

Allen Internetadressen liegt prinzipiell dieses Verfahren zu Grunde: Zunächst wird eine Verbindung zum DNS hergestellt, um die diesem Host-Namen zugeteilte IP-Adresse zu ermitteln. Ist das geschehen, wird mit dieser „nachgeschlagenen“ IP-Adresse die Verbindung zur gewünschten Gegenstelle, eine beliebige Internetpräsenz aufgebaut.

EDGE

EDGE (= Enhanced Data Rates for GSM Evolution) bezeichnet eine Technik, bei der die verfügbaren Datenraten in GSM-Mobilfunknetzen durch Einführung eines zusätzlichen Modulationsverfahrens erhöht werden. Mit EDGE werden GPRS zu EGPRS (Enhanced GPRS) und HSCSD zu ECSD erweitert.

EGPRS

EGPRS steht für "Enhanced General Packet Radio Service " und beschreibt einen auf GPRS beruhenden paketorientierten Datendienst, der durch EDGE-Technologie beschleunigt ist.

GPRS

GPRS ist die Abkürzung von "General Packet Radio Service" und ein Datenübertragungssystem von GSM2+ Mobilfunksystemen. GPRS-Systeme nutzen die Basisstationen der GSM-Netze für die Funktechnik und eine eigene Infrastruktur zur Vernetzung und zur Kopplung an andere IP-Netze, wie zum Beispiel dem Internet. Daten werden dabei paket-orientiert vermittelt, wobei das Internet Protokoll (IP) verwendet wird. GPRS stellt Datenraten von bis zu 115,2 KBit/s zur Verfügung.

GSM

GSM (= Global System for Mobile Communication) ist ein weltweit verbreiteter Standard für digitale Mobilfunknetze. GSM unterstützt außer dem Sprachdienst zur Telefonie, verschiedene Datendienste, wie Fax, SMS, CSD und GPRS. Abhängig von gesetzlichen Bestimmungen in den verschiedenen Ländern, werden die Frequenzbänder 900 MHz, 1800 MHz oder 850 MHz und 1900 MHz verwendet.

HSPDA, HSUPA (HSPA+)

HSDPA (=High Speed Downlink Packet Access) und HSUPA (=High Speed Downlink Packet Access) sind Erweiterungen des UMTS-Netzes, die höhere Übertragungsraten bei der Datenübertragung von der Basisstation zur Mobilstation (HSDPA) bzw. von der Mobilstation zur Basisstation (HSUPA) ermöglichen.

HTTPS

HTTPS (=HyperText Transfer Protocol Secure) ist eine Variante des bekannten HTTP, wie es von jedem Web-Browser zur Navigation und zum Datenaustausch im Internet verwendet wird. Bekannt ist die Eingabe: http://www.neuhaus.de.

Bei HTTPS ist dem ursprünglichen Protokoll eine zusätzliche Komponente zum Datenschutz hinzugefügt. Während HTTP-Daten ungeschützt in Klartext übertragen werden, werden HTTPS-Daten erst nach einem Austausch von Sicherheitszertifikaten verschlüsselt übertragen.

IP-Adresse

Jeder Host oder Router im Internet / Intranet hat eine eindeutige IP-Adresse (IP = Internet Protocol). Die IP-Adresse ist 32 Bit (= 4 Byte) lang und wird geschrieben als 4 Zahlen (jeweils im Bereich 0 bis 255), die durch einen Punkt voneinander getrennt sind.

Eine IP-Adresse besteht aus 2 Teilen: der Netzwerk-Adresse und der Host-Adresse.

Alle Hosts eines Netzes haben dieselbe Netzwerk-Adresse, aber unterschiedliche Host-Adressen. Je nach Größe des jeweiligen Netzes - man unterscheidet Netze der Kategorien Class A, B und C - sind die beiden Adressanteile unterschiedlich groß:

<table>
<tr><th></th><th>1. Byte</th><th>2. Byte</th><th>3. Byte</th><th>4. Byte</th></tr>
<tr><td>Class A</td><td>Netz-adresse</td><td colspan="3">Host-Adresse</td></tr>
<tr><td>Class B</td><td colspan="2">Netzadresse</td><td colspan="2">Host-Adresse</td></tr>
<tr><td>Class C</td><td colspan="3">Netzadresse</td><td>Host-Adresse</td></tr>
</table>

Ob eine IP-Adresse ein Gerät in einem Netz der Kategorie Class A, B oder C bezeichnet, ist am ersten Byte der IP-Adresse erkennbar. Folgendes ist festgelegt:

	Wert des 1. Bytes	Bytes für die Netzadresse	Bytes für die Host-Adresse
Class A	1-126	1	3
Class B	128-191	2	2
Class C	192-223	3	1

Rein rechnerisch kann es nur maximal 126 Class A Netze auf der Welt geben, jedes dieser Netze kann maximal 256 x 256 x 256 Hosts umfassen (3 Bytes Adressraum). Class B Netze können 64 x 256 mal vorkommen und können jeweils bis zu 65.536 Hosts enthalten (2 Bytes Adressraum: 256 x 256). Class C Netze können 32 x 256 x 256 mal vorkommen und können jeweils bis zu 256 Hosts enthalten (1 Byte Adressraum).

IP-Paket

Siehe Datagramm

IPsec

IP security (IPsec) ist ein Standard, der es ermöglicht, bei IP-Datagrammen die Authentizität des Absenders, die Vertraulichkeit und die Integrität der Daten durch Verschlüsselung zu wahren. Die Bestandteile von IPsec sind der Authentication Header (AH), die Encapsulating-Security-Payload (ESP), die Security Association (SA), der Security-Parameter-Index (SPI) und der Internet Key Exchange (IKE).

Zu Beginn der Kommunikation klären die an der Kommunikation beteiligten Rechner das benutzte Verfahren und dessen Implikationen wie z. B. Transport Mode oder Tunnel Mode.

Im Transport Mode wird in jedes IP-Datagramm zwischen IP-Header und TCP- bzw. UDP-Header ein IPsec-Header eingesetzt. Da dadurch der IP-Header unverändert bleibt, ist dieser Modus nur für eine Host-zu-Host-Verbindung geeignet.

Im Tunnel Mode wird dem gesamten IP-Datagramm ein IPsec-Header und ein neuer IP-Header vorangestellt. D. h. das ursprüngliche Datagramm wird insgesamt verschlüsselt in der Payload des neuen Datagramms untergebracht.

Der Tunnel Mode findet beim VPN Anwendung: Die Geräte an den Tunnelenden sorgen für die Ver- bzw. Entschlüsselung der Datagramme, auf der Tunnelstrecke, d. h. auf dem Übertragungsweg über ein öffentliches Netz bleiben die eigentlichen Datagramme vollständig geschützt.

MIB

Siehe SNMP

NAT (Network Address Translation)

Bei der Network Address Translation (NAT) - oft auch als IP-Masquerading bezeichnet - wird hinter einem einzigen Gerät, dem sog. NAT-Router, ein ganzes Netzwerk „versteckt". Die internen Rechner im lokalen Netz bleiben mit ihren IP-Adressen verborgen, wenn Sie nach außen über den NAT-Router kommunizieren. Für die Kommunikationspartner außen erscheint nur der NAT-Router mit seiner eigenen IP-Adresse.

Damit interne Rechner dennoch direkt mit externen Rechnern (im Internet) kommunizieren können, muss der NAT-Router die IP-Datagramme verändern, die von internen Rechnern nach außen und von außen zu einem internen Rechner gehen.

Wird ein IP-Datagramm aus dem internen Netz nach außen versendet, verändert der NAT-Router den IP- und den TCP-Header des Datagramms. Er tauscht die Quell-IP-Adresse und den Quell-Port aus gegen die eigene offizielle IP-Adresse und einen eigenen, bisher unbenutzten Port. Dazu führt er eine Tabelle, die die Zuordnung der ursprünglichen mit den neuen Werten herstellt.

Beim Empfang eines Antwort-Datagramms erkennt der NAT-Router anhand des angegebenen Zielports, dass das Datagramm eigentlich für einen internen Rechner bestimmt ist. Mit Hilfe der Tabelle tauscht der NAT-Router die Ziel-IP-Adresse und den Ziel-Port aus und schickt das Datagramm weiter ins interne Netz.

Netzmaske / Subnetz-Maske

Einem Unternehmens-Netzwerk mit Zugang zum Internet wird normalerweise nur eine einzige IP-Adresse offiziell zugeteilt, z. B. 134.76.0.0. Bei dieser Beispiel-Adresse ist am 1. Byte erkennbar, dass

es sich bei diesem Unternehmens-Netzwerk um ein Class B Netz handelt, d. h. die letzten 2 Byte können frei zur Host-Adressierung verwendet werden. Das ergibt rein rechnerisch einen Adressraum von 65.536 möglichen Hosts (256 x 256).

Ein so riesiges Netz macht wenig Sinn. Hier entsteht der Bedarf, Subnetze zu bilden. Dazu dient die Subnetz-Maske. Diese ist wie eine IP-Adresse ein 4 Byte langes Feld. Den Bytes, die die Netz-Adresse repräsentieren, ist jeweils der Wert 255 zugewiesen. Das dient vor allem dazu, sich aus dem Host-Adressenbereich einen Teil zu "borgen", um diesen zur Adressierung von Subnetzen zu benutzen. So kann beim Class B Netz (2 Byte für Netzwerk-Adresse, 2 Byte für Host-Adresse) mit Hilfe der Subnetz-Maske 255.255.255.0 das 3. Byte, das eigentlich für Host-Adressierung vorgesehen war, jetzt für Subnetz-Adressierung verwendet werden. Rein rechnerisch können so 256 Subnetze mit jeweils 256 Hosts entstehen.

Port-Nummer

Das Feld Port-Nummer ist ein 2 Byte großes Feld in UDP- und TCP-Headern. Die Vergabe der Port-Nummern dient der Identifikation der verschiedenen Datenströme, die UDP/TCP gleichzeitig abarbeitet. Über diese Port-Nummern erfolgt der gesamte Datenaustausch zwischen UDP/TCP und den Anwendungsprozessen. Die Vergabe der Port-Nummern an Anwendungsprozesse geschieht dynamisch und wahlfrei. Für bestimmte, häufig benutzte Anwendungsprozesse sind feste Port-Nummern vergeben. Diese werden als Assigned Numbers bezeichnet.

PPPoE

Akronym für Point-to-Point Protocol over Ethernet. Basiert auf den Standards PPP und Ethernet. PPPoE ist eine Spezifikation, um Benutzer per Ethernet mit dem Internet zu verbinden über ein gemeinsam benutztes Breitbandmedium wie DSL, Wireless LAN oder Kabel-Modem.

PPTP

Akronym für Point-to-Point Tunneling Protocol. Entwickelt von Microsoft, U.S. Robotics und anderen wurde dieses Protokoll entwickelt, um zwischen zwei VPN-Knoten (→ VPN) über ein öffentliches Netz sicher Daten zu übertragen.

Private Key (privater Schlüssel), Public Key (öffentlicher Schlüssel); Zertifizierung (X.509)

Bei asymmetrischen Verschlüsselungsalgorithmen werden 2 Schlüssel verwendet: ein privater (*Private Key*) und ein öffentlicher (*Public Key*). Der öffentliche Schlüssel dient zum Verschlüsseln von Daten, der private Schlüssel zum Entschlüsseln.

Der öffentliche Schlüssel wird vom zukünftigen Empfänger von Daten denen zur Verfügung gestellt, die die Daten verschlüsselt an ihn versenden werden. Der private Schlüssel ist nur im Besitz des Empfängers. Er dient zum Entschlüsseln der empfangenen Daten.

Zertifizierung:

Damit der Benutzer des (zum Verschlüsseln dienenden) öffentlichen Schlüssels sichergehen kann, dass der ihm übermittelte öffentliche Schlüssel wirklich von der Instanz stammt, die die zu versendenden Daten erhalten soll, gibt es die Möglichkeit der Zertifizierung: Die Überprüfung der Echtheit des öffentlichen Schlüssels und die damit verbundene Verknüpfung der Identität des Absenders mit seinem Schlüssel übernimmt eine zertifizierende Stelle (*Certification Authority - CA*). Dies geschieht nach den Regeln der CA, indem der Absender beispielsweise persönlich zu erscheinen hat. Nach erfolgreicher Prüfung signiert die CA den öffentlichen Schlüssel des Absenders mit ihrer (digitalen) Unterschrift. Es entsteht ein *Zertifikat*.

Ein X.509-Zertifikat stellt eine Verbindung zwischen einer Identität in Form eines 'X.500 Distinguished Name' (DN) und einem öffentliche Schlüssel her, die durch die digitale Signatur einer X.509 Certification Authority (CA) beglaubigt wird. Die Signatur - eine Verschlüsselung mit dem Signaturschlüssel - kann mit dem öffentlichem Schlüssel überprüft werden, die die CA dem Zertifikatsinhaber aushändigt.

Protokoll, Übertragungs-protokoll

Geräte, die miteinander kommunizieren, müssen dieselben Regeln dazu verwenden. Sie müssen dieselbe „Sprache sprechen“. Solche Regeln und Standards bezeichnet man als Protokoll bzw. Übertragungsprotokoll. Oft benutzte Protokolle sind z. B. IP, TCP, PPP, HTTP oder SMTP. TCP/IP ist der Oberbegriff für alle auf IP aufbauenden Protokolle.

Service Provider

Anbieter, Firma, Institution, die Nutzern den Zugang zum Internet oder zu einem Online-Dienst verschafft.

Spoofing, Anti-Spoofing

In der Internet-Terminologie bedeutet Spoofing die Angabe einer falschen Adresse. Durch die falsche Internet-Adresse täuscht jemand vor, ein autorisierter Benutzer zu sein.

Unter Anti-Spoofing versteht man Mechanismen, die Spoofing entdecken oder verhindern.

SNMP

SNMP (Simple Network Management Protokoll) ist ein weit verbreiteter Mechanismus zur zentralen Kontrolle und Steuerung von Netzwerk-Komponenten wie zum Beispiel Server, Router, Switches, Drucker, Computer usw.

SNMP definiert den Kommunikationsablauf und den Aufbau der Datenpakete. Zum Transport wird UDP über IP verwendet.

SNMP definiert nicht die Werte, die gelesen oder verändert werden können.

Dies geschieht in einer MIB (Management Information Base). Die MIB ist eine Beschreibungsdatei, in denen die einzelnen Werte tabellarisch aufgeführt werden. Die MIB ist jeweils spezifisch für eine bestimmte Netzwerkkomponente oder für eine Klasse von Komponenten, zum Beispiel Switches.

SNMP-Trap

SNMP-Trap ist eine Benachrichtigung die mittels SNMP Agent (Simple Network Management Protokoll) von einer Netzwerk-Komponente unaufgefordert versendet wird.

SSH

SSH (Secure SHell) ist ein Protokoll, das den gesicherten und verschlüsselten Datenaustausch zwischen Rechnern ermöglicht. Verwendet wird Secure SHell zum Fernzugriff auf die Eingabekonsole von LINUX- basierten Maschinen.

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung werden Daten mit dem gleichen Schlüssel ver- und entschlüsselt. Beispiele für symmetrische Verschlüsselungsalgorithmen sind DES und AES. Sie sind schnell, jedoch bei steigender Nutzerzahl nur aufwendig administrierbar.

TACACS+

TACACS+ (**T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem Plus) ist ein standardisiertes Protokoll, das der Kommunikation zwischen Clients und Servern innerhalb eines Netzwerks in den Bereichen Authentisierung, Autorisierung und Abrechnung dient. Beispielsweise kann - wie beim

TAINY xMOD - ein TACACS+-Server aufgesetzt werden, der zentral die Zugangsdaten für alle Endgeräte im Netzwerk verwaltet und stellvertretend für diese bei Anmeldeanfragen die Autorisierung des jeweiligen Interessenten vornimmt. Dabei leitet das Endgerät die empfangenen Anmeldedaten an den TACACS+-Server weiter, der die für die Autorisierung notwendigen Prüfungen vornimmt und das Ergebnis der Prüfungen zurück an das Endgerät meldet.

TCP/IP (Transmission Control Protocol/Internet Protocol

Netzwerkprotokolle, die für die Verbindung zweier Rechner im Internet verwendet werden.

IP ist das Basisprotokoll.

UDP baut auf IP auf und verschickt einzelne Pakete. Diese können beim Empfänger in einer anderen Reihenfolge als der abgeschickten ankommen, oder sie können sogar verloren gehen.

TCP dient zur Sicherung der Verbindung und sorgt beispielsweise dafür, dass die Datenpakete in der richtigen Reihenfolge an die Anwendung weitergegeben werden.

UDP und TCP bringen zusätzlich zu den IP-Adressen Port-Nummern zwischen 1 und 65535 mit, über die die unterschiedlichen Dienste unterschieden werden.

Auf UDP und TCP bauen eine Reihe weiterer Protokolle auf, z. B. HTTP (Hyper Text Transfer Protokoll), HTTPS (Secure Hyper Text Transfer Protokoll), SMTP (Simple Mail Transfer Protokoll), POP3 (Post Office Protokoll, Version 3), DNS (Domain Name Service).

ICMP baut auf IP auf und enthält Kontrollnachrichten.

SMTP ist ein auf TCP basierendes E-Mail-Protokoll.

IKE ist ein auf UDP basierendes IPsec-Protokoll.

ESP ist ein auf IP basierendes IPsec-Protokoll.

Auf einem Windows-PC übernimmt die WINSOCK.DLL (oder WSOCK32.DLL) die Abwicklung der beiden Protokolle.

(→ Datagramm)

UDP

Siehe TCP/IP

UMTS

UMTS (Universal Mobile Telecommunication System) ist ein Mobilfunknetz der 3. Generation, das deutlich höhere Datenübertragungsraten ermöglicht, als die GSM-Netze der 2. Generation. UMTS bietet neben der Sprachübertragung, IP-basierte Datenübertragung und SMS-Übertragung auch die Möglichkeit zu Übertragung von Videoanwendungen.

Mit Ausnahme des nordamerikanischen Raums verwendet UMTS ein Frequenzband bei 2100 MHz. In Nordamerika werden die Frequenzbänder bei 850 MHz und 1900 MHz genutzt, die auch für GSM-Netze verwendet werden.

VPN (Virtuelles Privates Netzwerk)

Ein Virtuelles Privates Netzwerk (VPN) schließt mehrere voneinander getrennte private Netzwerke (Teilnetze) über ein öffentliches Netz, z. B. das Internet, zu einem gemeinsamen Netzwerk zusammen. Durch Verwendung kryptographischer Protokolle wird dabei die Vertraulichkeit und Authentizität gewahrt. Ein VPN bietet somit eine kostengünstige Alternative gegenüber Standleitungen, wenn es darum geht, ein überregionales Firmennetz aufzubauen.

X.509-Zertifikat

Eine Art „Siegel“, welches die Echtheit eines öffentlichen Schlüssels (→ asymmetrische Verschlüsselung) und zugehöriger Daten belegt.

Damit der Benutzer eines zum Verschlüsseln dienenden öffentlichen Schlüssels sichergehen kann, dass der ihm übermittelte öffentliche Schlüssel wirklich von seinem tatsächlichen Aussteller und damit der Instanz stammt, die die zu versendenden Daten erhalten soll, gibt es die Möglichkeit der Zertifizierung. Diese Beglaubigung der Echtheit des öffentlichen Schlüssels und die damit verbundene Verknüpfung der Identität des Ausstellers mit seinem Schlüssel übernimmt eine zertifizierende Stelle (Certification Authority - CA). Dies geschieht nach den Regeln der CA, indem der Aussteller des öffentlichen Schlüssels beispielsweise persönlich zu erscheinen hat. Nach erfolgreicher Überprüfung signiert die CA den öffentlichen Schlüssel mit ihrer (digitalen) Unterschrift, ihrer Signatur. Es entsteht ein Zertifikat.

Ein X.509(v3)-Zertifikat beinhaltet also einen öffentlichen Schlüssel, Informationen über den Schlüsseleigentümer (angegeben als Distinguished Name (DN)), erlaubte Verwendungszwecke usw. und der Signatur der CA.

Die Signatur entsteht wie folgt: Aus der Bitfolge des öffentlichen Schlüssels, den Daten über seinen Inhaber und aus weiteren Daten erzeugt die CA eine individuelle Bitfolge, die bis zu 160 Bit lang sein kann, den sog. HASH-Wert. Diesen verschlüsselt die CA mit ihrem privaten Schlüssel und fügt ihn dem Zertifikat hinzu. Durch die Verschlüsselung mit dem privaten Schlüssel der CA ist die Echtheit belegt, d. h. die verschlüsselte HASH-Zeichenfolge ist die digitale Unterschrift der CA, ihre Signatur. Sollten die Daten des Zertifikats missbräuchlich geändert werden, stimmt dieser HASH-Wert nicht mehr, das Zertifikat ist dann wertlos.

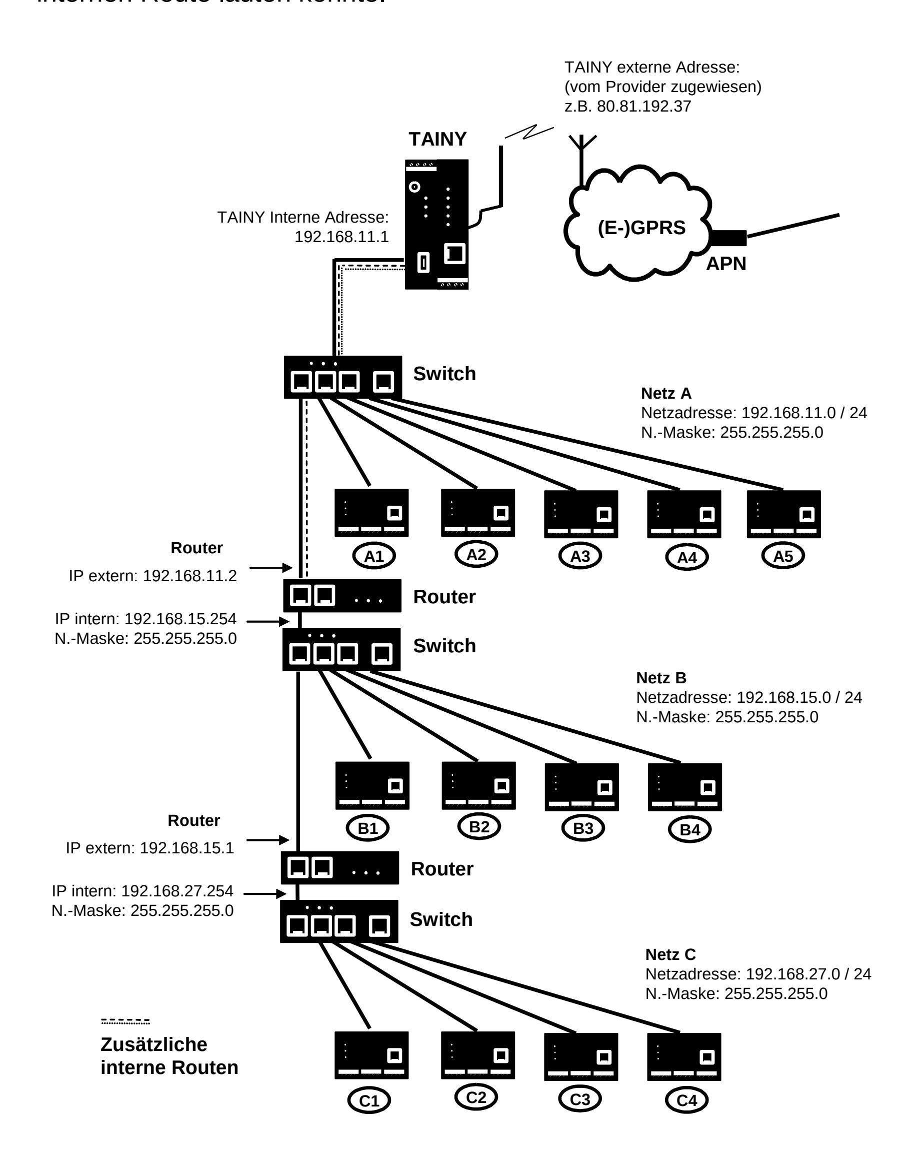
Der HASH-Wert wird auch als Fingerabdruck bezeichnet. Da er mit dem privaten Schlüssel der CA verschlüsselt ist, kann jeder, der den zugehörigen öffentlichen Schlüssel besitzt, die Bitfolge entschlüsseln und damit die Echtheit dieses Fingerabdrucks bzw. dieser Unterschrift überprüfen.

Durch die Heranziehung von Beglaubigungsstellen ist es möglich, dass nicht jeder Schlüsseleigentümer den anderen kennen muss, sondern nur die benutzte Beglaubigungsstelle. Die zusätzlichen Informationen zu dem Schlüssel vereinfachen zudem die Administrierbarkeit des Schlüssels.

X.509-Zertifikate kommen z.B. bei E-Mail-Verschlüsselung mittels S/MIME oder IPsec zum Einsatz.

Zusätzliche interne Routen

Die nachfolgende Skizze zeigt, wie in einem lokalen Netzwerk mit Subnetzen die IP-Adressen verteilt sein könnten, welche Netzwerk-Adressen daraus resultieren und wie die Angabe einer zusätzlichen internen Route lauten könnte.



Netz A ist an das TAINY xMOD angeschlossen und über dieses mit einem entfernten Netz verbunden. Zusätzliche interne Routen zeigen den Weg zu weiteren Netzen (Netz B, C), die über Gateways (Router) miteinander verbunden sind. Für das TAINY xMOD sind bei dem gezeigten Beispiel die Netze B und C beide über das Gateway 192.168.11.2 und die Netzwerkadresse 192.168.11.0/24 erreichbar.

<table>
<tr><th colspan="6">Netz A</th></tr>
<tr><td>Rechner</td><td>A1</td><td>A2</td><td>A3</td><td>A4</td><td>A5</td></tr>
<tr><td>IP-Adresse</td><td>192.168.11.3</td><td>192.168.11.4</td><td>192.168.11.5</td><td>192.168.11.6</td><td>192.168.11.7</td></tr>
<tr><td>Netzwerk-Maske</td><td>255.255.255.0</td><td>255.255.255.0</td><td>255.255.255.0</td><td>255.255.255.0</td><td>255.255.255.0</td></tr>
<tr><th>Netz B</th><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Rechner</td><td>B1</td><td>B2</td><td>B3</td><td>B4</td><td rowspan="7">Zusätzliche interne Routen:
Netzwerk:
192.168.15.0/24
Gateway:
192.168.11.2
Netzwerk:
192.168.27.0/24
Gateway:
192.168.11.2</td></tr>
<tr><td>IP-Adresse</td><td>192.168.15.3</td><td>192.168.15.4</td><td>192.168.15.5</td><td>192.168.15.6</td></tr>
<tr><td>Netzwerk-Maske</td><td>255.255.255.0</td><td>255.255.255.0</td><td>255.255.255.0</td><td>255.255.255.0</td></tr>
<tr><th>Netz C</th><td></td><td></td><td></td><td></td></tr>
<tr><td>Rechner</td><td>C1</td><td>C2</td><td>C3</td><td>C4</td></tr>
<tr><td>IP-Adresse</td><td>192.168.27.3</td><td>192.168.27.4</td><td>192.168.27.5</td><td>192.168.27.6</td></tr>
<tr><td>Netzwerk-Maske</td><td>255.255.255.0</td><td>255.255.255.0</td><td>255.255.255.0</td><td>255.255.255.0</td></tr>
</table>

17 Technische Daten

17.1 TAINY HMOD

Schnittstellen	Applikations-Schnittstellen	2-Port-Version: 2x 10/100 Base-T (RJ45 plug) Ethernet IEEE802, 10/100 Mbit/s 5-Port-Version: 5x 10/100 Base-T (RJ45 plug) Ethernet IEEE802, 10/100 Mbit/s
	Service Schnittstelle	USB-A (reserviert für spätere Anwendungen)
Sicherheits-Funktionen	VPN	IPsec (nur TAINY HMOD-V3-IO) Etwa 10 VPN-Tunnel
	Firewall	Stateful Inspection Firewall Anti-Spoofing Port Weiterleitung
Weitere Funktionen		DNS Cache, DHCP-Server, NTP, Remote Logging, Verbindungsüberwachung, Alarm-SMS, SNMP, TACACS+
Management		Web-basierte Administrations-Oberfläche, SSH-Konsole
Funkverbindung	Frequenzbänder	UMTS/HSPA+: 800/850, 900, 1900, 2100 MHz GSM/GPRS/EDGE: 850, 900, 1800, 1900 MHz
	HSPA+	HSDPA/HSUPA Datenraten: DL: 7.2 / 14.4 Mbps, UL: 2.0 / 5.76 Mbps Concurrent data rate: DL: 7.2 Mbps, UL: 5.76 Mbps
	UMTS	DL: max. 384 kbps, UL: max. 384 kbps
	EDGE (EGPRS)	EDGE class 12: DL: max. 237 kbps, UL: max. 237 kbps
	GPRS	GPRS class 12: DL: max. 85.6 kbps, UL: max. 85.6 kbps
	CSD / MTC	CSD data transmission 14.4 kbps, V.110
	SMS (TX)	Punkt zu Punkt, MO (abgehend)
	Antennen-anschlüsse	2 Anschlüsse: Impedanz nominal: 50 Ohm, Buchse: SMA
Umwelt-bedingungen	Temperatur-bereich	Betrieb: -40 °C bis +70 °C *) Lagerung: -40 °C bis +85 °C *) Automatische Abschaltung des Funkmoduls bei kritischer Temperatur.
	Luftfeuchte	0-95 %, nicht kondensierend
Gehäuse	Ausführung	Hutschienengehäuse
	Material	Kunststoff
	Schutzklasse	IP20
	Abmessungen	2-Port-Version: 114,5 mm x 45 mm x 99 mm 5-Port-Version: 114,5 mm x 67 mm x 99 mm

	Gewicht	2-Port-Version: ca. 280g 5-Port-Version: ca. 400g
Konformität	CE	Ja
	R&TTE	Konform zur Richtlinie 99/05/EC Angewandte Normen: EN301 511 v.9.0.2, EN301908-1/-2 v.4.2.1
	HSPA+/UMTS/ GSM/EGPRS-Modul	Konform zu GCF, PTCRB
	EMV/ESD	Angewandte Normen: EN 301 489-1 v.1.8.1, EN 301 489-7 v.1.3.1, EN 61000-6-2:2005
	Elektrische Sicherheit	Angewandte Norm: EN 60950-1:11-2006/A1:2010
	Umwelt	Das Gerät entspricht den europäischen Richtlinien ROHS und WEEE.
Spannungs-versorgung	Eingangs-spannung	nominal 12-60 VDC, min. -10%, max +20%
	Leistungs-aufnahme	Typisch 4,4 W bei 12 V Typisch 4,0 W bei 24 V Typisch 5,5 W bei 60 V
	Stromaufnahme	450mA bei 12V und 100mA bei 60V I_{Burst} = 1,26A

17.2 TAINY EMOD

Schnittstellen	Applikations-Schnittstellen	2-Port-Version: 2x 10/100 Base-T (RJ45 plug) Ethernet IEEE802, 10/100 Mbit/s 5-Port-Version: 5x 10/100 Base-T (RJ45 plug) Ethernet IEEE802, 10/100 Mbit/s
	Service Schnittstelle	USB-A (reserviert für spätere Anwendungen)
Sicherheits-Funktionen	VPN	IPsec (nur TAINY EMOD-V3-IO)
	Firewall	Stateful Inspection Firewall Anti-Spoofing Port Weiterleitung
Weitere Funktionen		DNS Cache, DHCP-Server, NTP, Remote Logging, Verbindungsüberwachung, Alarm-SMS, SNMP, TACACS+
Management		Web-basierte Administrations-Oberfläche,ssh-Konsole
Funkverbindung	EDGE / GPRS	EDGE Multislot class 12 / EDGE Multislot class 12
	Coding schemes GSM Module	CS-1, CS-2, CS-3, CS-4 EGPRS (EDGE) / Quad band
	EDGE (EGPRS)	Multislot Class 12 Mobile Station Class B Modulation and Coding Scheme MCS 1 – 9
	GPRS	Multislot Class 12 Full PBCCH support Mobile Station Class B Coding Scheme 1 – 4
	EDGE / GPRS	Während der Datenübertragung über EGPRS oder GPRS wählt das Gerät automatisch zwischen folgenden Klassen aus: • von EGPRS Multislot Class 12 (4Tx slots) bis EGPRS Multislot Class 10 (2Tx slots), • von EGPRS Multislot Class 10 (2Tx slots) bis EGPRS Multislot Class 8 (1Tx), • von GPRS Multislot Class 12 (4Tx slots) bis GPRS Multislot Class 8 (1Tx) • von GPRS Multislot Class 10 (2Tx slots) bis GPRS Multislot Class 8 (1Tx)
	CSD / MTC	V.110, RLP, non-transparent 2.4, 4.8, 9.6, 14.4kbps
	SMS (TX)	Punkt zu Punkt, MO (abgehend)

	Max. Sendeleistung (gemäß Ausgabe 99, V5)	Class 4 (+33dBm ±2dB) for EGSM850 Class 4 (+33dBm ±2dB) for EGSM900 Class 1 (+30dBm ±2dB) for GSM1800 Class 1 (+30dBm ±2dB) for GSM1900 Class E2 (+27dBm ± 3dB) for GSM 850 8-PSK Class E2 (+27dBm ± 3dB) for GSM 900 8-PSK Class E2 (+26dBm +3 /-4dB) for GSM 1800 8-PSK Class E2 (+26dBm +3 /-4dB) for GSM 1900 8-PSK
	Antennen-anschluss	Impedanz nominal: 50 Ohm, Buchse: SMA
Umwelt-bedingungen	Temperatur-bereich	Betrieb: -20 °C bis +60 °C *) Lagerung: -40 °C bis +85 °C *) Automatische Abschaltung des Funkmoduls bei kritischer Temperatur.
	Luftfeuchte	0-95 %, nicht kondensierend
Gehäuse	Ausführung	Hutschienengehäuse
	Material	Kunststoff
	Schutzklasse	IP20
	Abmessungen	2-Port-Version: 114,5 mm x 45 mm x 99 mm 5-Port-Version: 114,5 mm x 67 mm x 99 mm
	Gewicht	2-Port-Version: ca. 280g 5-Port-Version: ca. 400g
Konformität	CE	Ja
	R&TTE (GSM)	Konform zur Richtlinie 99/05/EC Angewandte Normen: EN301 511 v.9.0.2, EN301908-1/-2 v.4.2.1
	GSM/EGPRS-Modul	Konform zu GCF, PTCRB
	EMV/ESD	Angewandte Normen: EN 301 489-1 v.1.8.1, EN 301 489-7 v.1.3.1, EN 61000-6-2:2005
	Elektrische Sicherheit	Angewandte Norm: EN 60950-1:11-2006/A1:2010
	Umwelt	Das Gerät entspricht den europäischen Richtlinien ROHS und WEEE.
Spannungs-versorgung	Eingangs-spannung	nominal 12-60 VDC, min. -10%, max +20%
	Leistungs-aufnahme	Typisch 4,4 W bei 12 V Typisch 4,0 W bei 24 V Typisch 5,5 W bei 60 V
	Stromaufnahme	450mA bei 12V und 100mA bei 60V I_{Burst} = 1,26A